□특집□

면역학 기반의 외부침입 탐지 시스템[1)]

최 종 욱†

◈ 목 차 ◈

1. 인터넷의 활성화와 침입탐지 시스템

미국에서 5천만명의 사용자를 확보하는데 걸리는 시간을 따져 보았더니 전화는 25년, 라디오는 38년, TV는 13년, 케이블 TV는 10년이 걸렸는데 인터넷은 불과 5년이 걸렸다는 통계나 인터넷 거래가 100일마다 2배가 된다는 통계 등을 감안하면 이제 인터넷 세상은 피할 수 없게 되었다. 인터넷 통계로 유명한 포레스터(Forrester)사에 의하면 98년초 미국에서 인터넷을 사용하여 물건을 사본 적이 있는 사용자는 6개월 전 740만명에서 1000만명으로 증가하였다. 또한 미국 가정의 43%가 집에 PC를 가지고 있으며 전체 가정의 25%가 지속적으로 인터넷에 접속하고 있다고 한다. 이미 국내에서도 98년 전자 우편 사용건수가 일반 우편 사용 건수를 추월하였다는 통계가 나와있고, 이미 99년말 인터넷 인구가 연초의 예상치인 600만명을 훨씬 넘어서는 1,000 만명을 초과하였다는 보도가 있었다.

이처럼 인터넷 전자 상거래가 급증하고 네트워크 이용이 크게 증가하면서 외부 침입 및 내부자의 중요 기밀 문서 외부 유출이 중요한 사회적 문제로 떠오르고 있다. 인터넷 전자 상거래는 생활의 편리성을 떠나 이제 기업과 기관, 사회와 국가의 경쟁력을 좌우하는 사회적인 인프라로 자리 잡고 있다. 지난 2월 7일을 전후하여 yahoo, amazon, buy, e-bay, CNN, e-trade 등의 미국의 유명 사이트들이 해커들의 장난에 의해 서비스를 중단하는 사건이 있었다. 해커들의 침입은 잠시동안의 서비스 중단으로만 끝나는 것이 아니다. 막대한 자원의 손실과 사회적 신뢰의 손상으로 이어질 수 있다는 점에서 심각한 사회문제가 되고 있다.

따라서 인터넷을 통한 거래와 정보의 교환, 상거래, 물류정보의 유통, 그리고 내부에 저장된 정보의 보호를 위한 탐지/적발 시스템을 개발할 필요가 있다. 현재 세계적으로 네트워크 정보 보안 시스템 기술이 경쟁적으로 개발되고 있으나 아직은 단일 시스템, 혹은 계층형 시스템에서의 외부 침입 탐지 시스템을 개발하고 있어 빠르게 분산 시스템으로 옮겨가고 있는 실제 컴퓨터 환경을 따라 잡지 못하고 있다.

이러한 분산 시스템에서의 외부침입 탐지 기술을 개발하기 위해 외부에서 침입한 병원균을 효과적으로 탐지/파괴하는 인체 면역 시스템을 응용하려는 것이 최근 활발하게 연구되고 있는 면역 메커니즘 기반의 침입 탐지 시스템이다. 이는 인간의 면역 메커니즘이 신체에 침입하는 이물질을 구분해내고 이를 퇴치하기 위해 자기 복제나 다른 유전자들과 상호작용을 한다는 점에서, 그리고

1) 본 연구는 과학재단 특정기초연구(1999-2-511-001-3)의 지원에 의해 수정되었음.

† 종신회원 : 상명대학교 정보통신학부 정보과학과 부교수

가장 유연하고 효과적이면서 외부침입에 강인한 침입 탐지 및 퇴치 시스템이라는 점에서 네트워크 보안 시스템에 응용하는 것이 효과적인 시스템 구현에 필요하다고 믿기 때문이다.

2. 기존 침입탐지 시스템의 문제점

일반적으로 해커로부터 시스템을 보호하기 위해서 방화벽 (Firewall)만으로는 충분하지 못하다[19]. 방화벽은 기본적으로 전체를 막고 난 뒤 몇몇 필요 요건을 만족시키는 것들만을 출입시키는 시스템이다. 방화벽을 설치할 때 제일 먼저 하는 일은 모든 통신을 중단시키고 방화벽을 통과할 수 있는 몇 가지 특정의 '규칙'을 입력하는 것이다. 이 때문에 대부분 기업 네트워크에서는 UDP와 ICMP 데이터 그램, 외부에서 들어오는 TCP연결을 중시시키고 외부로 나가는 TCP만 열어 놓는 경우가 많다. 즉, 방화벽은 단순한 울타리에 불과한 것이며 울타리를 부시려는 사람이나 울타리를 교묘하게 통과한 경우, 혹은 내부에서 중요 문서를 밖으로 유출하는 경우를 막지 못한다.

결론적으로 방화벽은 능동적인 방어 시스템이 아니다. 이에 반해 IDS는 방화벽이 감지못하는 공격에 대해 인식할 수 있으며 더 나아가서는 이전에 경험하지 못한 공격에 대해서도 이를 감지, 퇴치할 수는 능동적인 시스템이다. 기존 방화벽 시스템의 결함에 대해 설명을 할 때 Cold Fusion을 자주 예로 들고 있다. Cold Fusion은 Allaire라는 기업에서 만든 전자 상거래 플랫폼 시스템이다. 이 Cold Fusion에 들어 있던 결함(Bug) 때문에 99년 4월 많은 사이트에 해커 침입이 있었다고 보도되었다. 그런데 이 시스템을 사용하는 웹사이트들은 웹 서버에 접근하기 위해서는 80번 포트만 사용하도록 하는 방화벽을 사용하였고 그럼에도 불구하고 결국 웹서버는 해킹을 당하였다[19]. 이처럼 방화벽만으로는 공격에 대한 방어를 할 수 없다. 반면에 IDS는 시스템에 남겨진 흔적(signature)을 가지고 공격을 탐지한다. 더구나 기업 시스템에 가해지는 재정적인 손실의 80%는 외부 해커보다는 내부적인 공격 때문이고, 이러한 내부적인 공격은 방화벽을 가지고는 탐지가 불가능하다. 내부적인 공격에 대해서는 IDS를 사용할 수밖에 없다.

침입 탐지 시스템에 있어 핵심기술은 행위 판별(Behavior Classification)과 자료 축소(Data Reduction) 기술이다. 행위 판별은 주어진 일련의 행위들에 대해 이것이 침입인지 아닌지를 판단하는 문제이고, 자료 축소는 수 메가바이트에 이르는 방대한 양의 데이터를 의미 있는 소규모의 자료 집단으로 줄여 나가는 과정이다. 대체적으로 침입 탐지에서는 규칙 기반 시스템(Rule-based System)과 신경망[9] 또는 통계적 분류 시스템의 방법을 도입하여 사용하고 있다[11][14]. 기존에 사용된 규칙기반 시스템이나 신경망, 통계적인 분류시스템은 많은 양의 초기 학습을 필요로 하며, 시스템의 수명동안 지속적으로 시스템의 유지보수를 위해 많은 노력이 필요하다는 문제점 외에도 새로운 공격 유형에는 약하다는 단점이 있다.

규칙 기반 침입 탐지 시스템의 대표적인 예로는 IDES 시스템이 있다. 이 시스템은 대상 시스템의 취약성 및 보안 정책, 그리고 과거의 침입들에 대한 지식을 규칙 데이터베이스에 가지고 있다. 시스템에 침입이 발생할 경우, 탐지 시스템은 침입에 대한 규칙베이스(Rule Base)에 의해 현 시스템이 침입 당했는지 여부를 분류하게 된다. IDES시스템은 과거의 침입에 대해 이를 기억하고 있다는 중요한 특징이 있다. 이것은 침입 탐지 시스템의 성능 향상에 있어 매우 중요한 특징으로 대부분의 새로운 침입 형태들은 기존 형태의 부분적인 변형이기 때문에 정확성이 높다.

규칙기반 IDS의 경우 초기의 규칙 기반 마련을 위해 보안분야의 높은 전문성을 가진 전문가의

지식을 필요로 한다. 이는 오랜 시간과 막대한 개발비를 요하는 작업이다. 게다가 어떤 전문가라 할지라도 시스템의 모든 취약성에 대해 알 수 없으며, 많은 기존 시스템의 약점들 간의 상호작용으로 생겨나는 취약성에 대해서는 더더욱 이를 발견해 낼 수 없다는 문제점이 있다. 만일 시스템의 프로파일상의 중요한 변화가 일어난다면, 규칙 기반 시스템의 경우 새로운 침입 가능성에 대비하여 규칙 기반을 새로이 설계해야만 한다. 이는 오류 발생 가능성이 매우 높은 작업으로 새로운 규칙이 기존의 규칙들과 충돌하는 내용일 수도 있다. 이러한 문제들은 시스템 운영자에게 현재 규칙의 운영 및 유지를 어렵게 하여, 결과적으로 침입 탐지 시스템의 과거 정보에 의존적이 되도록 한다.

Headye와 Luger 등은 분류 시스템(Classifier System) 기술을 이용한 침입탐지 기술을 제안하였다[8]. 이것은 네트워크 패킷 정보에 관한 매트릭스들을 구축한 후 이들로부터 네트워크에 관한 분류를 어떻게 할 수 있는지를 추론하게 된다. 그러나 이러한 접근법은 크게 두 가지의 한계점을 지니고 있다. ATM이나 FDDI 백본과 같이 많은 컴퓨터들이 빠른 속도의 네트워크로 연결되어 있는 경우 성능의 저하가 현격하다는 것과 네트워크의 상태를 판단하는데 사용되는 정보가 패킷의 헤더데이터에 국한되어 있다는 점이다. 헤더로부터 추출한 정보로서는 행위의 특징을 처리할 수 없기 때문에 실제적으로 분류에 필요한 유용한 정보를 추출하기에는 역부족이다. 예를 들어 합법적인 메일 포트를 통하여 침입이 이루어질 경우 이 방법으로는 침입을 구분해 낼 수 없게 된다.

Kumar와 Spaffod에 의해 제안된 패턴 매칭 기법에 기반한 접근법은 시스템상에 요구되는 유연성의 향상에 초점이 맞추어져 있지만 학습능력을 갖추지 못하였다는 단점을 가지고 있다[14]. 이들은 시스템상에 나타나는 현상들에 근거하여 침입을 어떻게 분류하는 지를 보여주고 있다. 여기서의 각 패턴들은 시스템 상태들간의 의존도를 인코딩하고 있는 것이다. 이러한 접근법은 침입을 탐지하는 강력한 방법이나 사전에 만들어진 패턴들에 의존적이라는 단점 또한 가지고 있다. 즉, 패턴 자체가 완전하지 못할 경우 시스템의 방어에 커다란 허점이 나타나게 되는 것이다. 그리고 보안 정책이나 시스템 운영상에 변화가 있을 경우 패턴들을 다시 만들어야 한다는 문제점이 있다.

현재까지 제시된 침입 탐지 시스템들은 몇 가지 문제점들을 공통적으로 가지고 있는데 이 중 가장 두드러진 문제점은 시스템 부하에 관한 것이다. 이를 해결하기 위해 별도의 침입 탐지 모듈에 의해 네트워크 전체가 분석되도록 하고 있다. 다음으로는 데이터의 축소문제가 있다. 감사 데이터(Audit Trail)를 분석하기 위해서는 시스템 커널이 시스템 상에서 이루어지는 모든 행동들에 대해 감사 정보를 만들어 내야 하는 데, 그 양이 엄청나며 분석 작업에는 시스템의 디스크 용량이나 CPU Time의 엄청난 소모가 필요하다. 실제적으로 영국의 University College London(UCL)에서도 침입탐지 시스템을 개발하기 위해 기존의 신경망 기법과 유전자 알고리즘, 그리고 전문가 시스템 기술을 이용하였으나 규모 문제(Scalability)에 부딪쳐 사업이 중단되었다. 이는 소규모 시제품 시스템에서는 인공지능 기법이나 분류기법, 유전자 알고리즘이 효과적으로 적용되지만 실제 네트워크 시스템에서는 그 규모 문제 때문에 운영이 어려워지기 때문이다.

3. 인체 면역 시스템

새로운 공격 유형에 대한 탐지력을 높이기 위해 최근 인체 면역 메커니즘을 적용하려는 시도들이 나타나고 있다. 인체 면역 메커니즘은 이물질 구분과 자기 복제 등의 장치를 이용하여 외부 침입으로부터 방어를 하고 있으며 외부 침입 탐

지 시스템에서 필요한 분산화, 자기 조직화(Self-Organization), 경량화(Lightweight)라는 조건을 만족시킬 수 있어 효율적인 외부침입 탐지 및 적발 시스템을 구현할 수 있을 것으로 예상하고 있다.

3.1 임파구의 생성과 소멸

인체의 면역은 선천성 면역(innate)과 후천성 면역(specific)으로 나누어진다. 선천성 면역은 각 세균을 구분하는데 있어 그 능력에 상당한 한계를 갖는 면역 시스템으로 대부분의 세균성 세포에 대해 다분히 고정된 반응을 보인다. 선천성 면역 시스템은 세균에 대해 일차 방어로서 의미를 갖는다. 이에 반해 후천성 면역 시스템은 훨씬 높은 적응성을 가지고 있어 다양한 세균의 형태나 특이성에도 반응할 수 있다. 후천성 면역은 임파구와 그 산출물인 항체로 이루어지며 특별한 면역적 반응을 유도하는 외래 물질을 항원(anti-gen)이라고 부른다. 따라서 인간의 면역시스템에서는 선천성 면역시스템이 일차적인 방어시스템 역할을 하고, 후천적인 면역 시스템 활성화를 유도한다. 후천성 면역 시스템은 다양한 항원에 대해 특수한 반응을 수행함으로서 세균을 제거하게된다. 이들 두 시스템이 상호 보완적으로 통합되면서 인체는 외부로부터의 세균 침입을 방어하게된다.

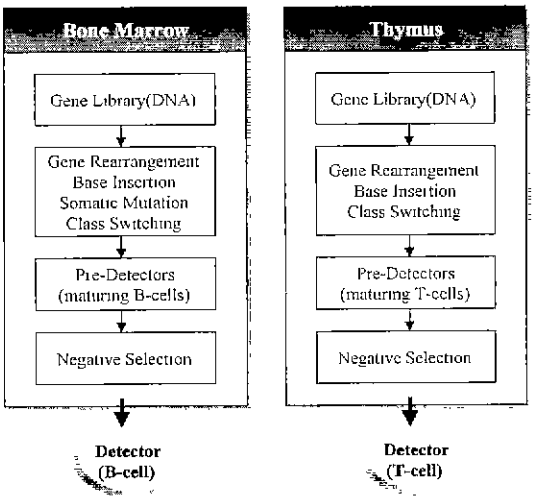
모든 면역 시스템은 외래 항원(anti-gen)을 인식하면서부터 시작된다. 항원은 외부로부터의 이물질이나 세균세포이며 이러한 항원을 특별히 인식할 수 있는 임파구가 활성화된다. 이에 따라 면역학적 기능인 항원의 제거가 이루어진다. 임파구는 크게 B-cell과 T-cell 두 가지로 분류되는데, B-cell은 혈청 속에서 항독 작용 혹은 살균작용을 하는 항체 세포이고 T-cell은 항원을 죽이기도 하며 B-cell의 성장을 억제하거나 도와주는 세포이다. B-cell과 T-cell 모두 그들 나름대로 유일한 유전자 구조를 가지고 있다. B-cell과 T-cell은 모두

〈표 1〉 면역 시스템의 모듈

명 칭	기 능
B-cell	Bone Marrow에서 생산되는 것으로 항원을 바인딩할 수 있는 세포
T-cell	Thyms에서 생산되며 B-cell이 항원을 바인딩 하는 것을 도우며 B-cell의 효율성 여부를 판단하여 B-cell을 제거시키기도 한다.
Pre-detector	이는 Negative selection과정을 통과하기 전의 Detector로 항원에 대한 Binding 능력이 검증되지 않은 상태의 탐지기이다.
Memory Cell	기억세포는 Detector가 포함하고 있는 기능으로 항원에 대한 Binding 기록을 저장한다.
Anti-Antibody	항항체는 B-cell이나 T-cell과 같은 항체의 조절 역할을 하며 정상적인 자원을 Binding하려고 하는 항체를 제거한다.
Antigen	시스템에 침투하는 항원으로 침입자로 여겨진다.
Bone Marrow & Thyms	Bone Marrow와 Thyms는 각각 B-cell과 T-cell을 생성한다.
Gene Library	이는 네트워크 침입에 대한 효율적인 바인딩 방법을 저장하며 이는 다른 IDS의 생성에 관여한다.
Negative Selection	침입에 대해 정상적으로 반응을 보이지 못하는 Cell을 신속하게 제거시킨다.
Clonal Selection	효과적인 탐지능력을 지닌 Cell을 복제한다.
Primary IDS	이는 Gene Library, Negative Sclection, Clonal Selection을 포함하며, Secondary IDS을 총괄적으로 관리한다.
Secondary IDS	로컬 서버에 존재하며, 네트워크 패킷의 이상이 탐지되며 자원에 대한 보안 분석을 수행한다.

DNA(유전자 라이브러리)의 체인으로써 표현되며 각 체인은 변동 영역과 고정 영역을 가지고 있다. 변동 영역의 유전자들은 임파구에 따라 모두 각기 다른 구조를 가지며 이러한 차이점 때문에 각 항원들에 대한 임파구의 바인딩(binding)부분이 달라진다[7][8]. 고정 영역에서의 유전자들은 변동이 없으며 B-cell 항체 수용체(receptor)가 항원의 에피토프(epitope)를 바인딩 할 때 다양한 생물학적 효력을 발휘한다. 항체(anti-body)가 항원(anti-gen)을 바인딩할 때 전체를 다하는 것이 아니고 특정 부분만 바인딩하게 되는데 이 부분을 결정자(determinant) 혹은 에피토프(epitope)라 부른다.

B-cell과 T-cell은 각각의 골수(bone marrow)나 흉선(thymus)에서 생긴다. 골수와 흉선에서 각각 B-cell과 T-cell의 영역에 해당하는 몇몇의 유전자 라이브러리들(gene libraries)은 B-cell과 T-cell의 수용기(receptor)를 만들 수 있는 후보 유전자들을 가지고 있다. 특정 수용기는 유전자 라이브러리로부터 임의적으로 유전자 군을 뽑아서 이들을 조합함으로서 만들어진다. 다양한 수용기를 만들어 내기 위해서는 수용기 생성 단계에서 순차적으로, 그리고 점진적인 생성과정이 이루어진다.



(그림 1) T-Cell과 B-Cell의 성장

골수와 흉선을 떠나기 전에 성장한 B-cell과 T-cell은 마지막 시험과정인 negative selection을 통과한다. B-cell과 T-cell의 숙성과정에서 여러 가지 유전자 운영 메커니즘에 의해 완전히 새로운 세포 수용체가 만들어진다. 따라서 임의적으로(randomly) 생성된 수용기들이 자신의 세포 에피토프와 결합할 수 있는 가능성도 있다. 이러한 경우를 방지하기 위해 성장하고 있는 B-cell과 T-cell이 골수와 흉선을 순환하고 있는 자기 세포와 바인딩하려고 할 때는 몸속으로 보내기 이전에 제거된다.

성장한 B-cell과 T-cell은 마지막 단계인 negative selection을 거치게 되면 골수와 임파구로부터 방출되어 몸 속을 순환하게 된다. B-cell의 항체는 항원들을 찾아내게 되면 이를 바인딩하고 직접적이거나 간접적으로 활성화된다. 만약 B-cell 항체의 수용체가 임계치를 넘는 강한 친화력을 가지고 항원의 에피토프를 바인드할 때 직접적인 활성화가 된다. 그러나 B-cell이 임계치 이하의 약한 친화력을 항원의 에피토프와 바인딩할 할 때는 활성화되기 위해 T-cell이나 Major-Histocompatibility Complex(MHC) 분자의 도움을 필요로 한다.

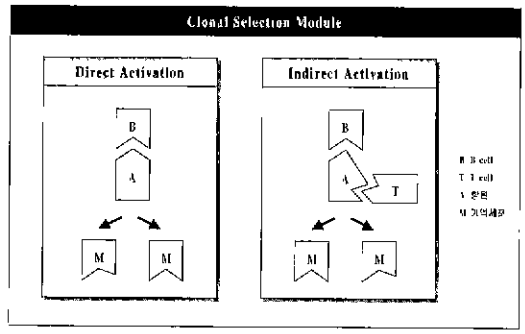
MHC 분자들은 B-cell의 활성화를 돕기 위한 두 가지 기능을 가지고 있다. 첫 번째는, MHC 분자는 특별히 세포 내에 숨어있는(세포의 표면에서 보이지 않는) 항원들과 바인딩한다. 두 번째는, MHC 분자는 바인딩 한 항원 부분을 B-cell의 표면으로 옮겨놓는다. 만약 약한 친화력을 지닌 B-cell 항체의 수용체가 항원의 에피토프를 바인딩 할 때, MHC 분자는 세포 내에 숨어있는 내부 세포를 찾기 위하여 노력한다. MHC 분자가 그러한 항원 세포들을 찾았을 때 B-cell의 표면으로 그것을 전송한다. T-cell의 수용체는 B-cell 표면에 있는 MHC 분자를 인지하도록 유전적으로 구조화되어 있다. T-cell이 강한 친화성을 가지고 MHC 분자를 바인딩 할 때 T-cell은 Bell-cell에게 화학

적 신호를 보내어 B-cell이 활성화되고, 성장하고 특화되도록 한다.

그렇다면 T-cell이 어떻게 하여 B-cell의 활성화를 결정하는가? B-cell과 T-cell의 중요한 차이 한 가지는 오직 B-cell만이 골수에서 성장할 때 다양성을 증가시키기 위하여 매우 높은 돌연 변이율을 가지고 신체 돌연변이를 수행한다는 것이다. B-cell은 T-cell보다 매우 다양하고 새로운 수용체를 갖게된다. 게다가 골수는 신체 부위에 분산되어 있지만 흉선은 신체의 중앙에 위치하고 있다. 따라서 대부분의 자가 세포가 흉선을 통과하게 되며, 흉선에서의 negative selection 과정을 통과한 이들 세포들은 골수를 통과한 세포들 보다 더 신뢰성 있어진다. 그러므로, 약한 친화성을 가진 B-cell 활성화는 최종적으로 T-cell에 의해서 결정되어 진다.

T-cell의 도움이 있건 없건 간에 B-cell이 활성화되어지고 이러한 활성화는 즉시 유전자 복제로 이어진다. 활성화된 B-cell은 다수의 복제세포로 나누어지고 이들은 부모 B-cell과 똑 같은, 혹은 돌연변이된 항원-바인딩 특성을 갖게된다. 만약 일정한 시간 동안에 B-cell이 활성화되지 못하면 빠르게 제거된다. 따라서 현재의 항원에 대해서는 가장 적합한 항체들만이 살아남는다. 항원은 지속적인 변화를 하기 때문에 항원 탐지 효율은 복제선택을 통한 B-cell항체의 진화과정에 의해 유지된다. 이러한 메모리 효과 때문에 이전에 구분된(Identified) 항원은 다음번 침입에 더욱 빠르게 탐색될 수 있다. (그림 3)에서는 유전자 복제에 의한 기억세포들의 생성을 보여준다.

항항체들(anti- antibodies)인 유전자형 항체들은 항체의 수용체들을 활성화시킬 수 있다. 면역 시스템은 항원과 항항체로 하여금 항체에게 바인딩할 수 있도록 하며, 승리한 항항체가 항체와 항원사이에서 발생하는 바인딩을 진압할 수 있도록 한다. 항원에 대한 유전적 항체의 진압은 면역 반응의 적당한 수준을 조절하는데 도움을 준다. 면역학자인 Jern은 유전적 항체의 역할을 이해하는데 기본을 두고 있는 면역 네트워크 이론을 제안하였다. 그는 면역 시스템이 임파구의 기능적인 네트워크이며 어떠한 순간에 이 네트워크는 항체와 항원의 내부 상호작용의 동적인 상태를 가진다고 보았다. 항원에 대한 식별과 유전적 항체에 의한 진압의 끊임없는 반복은 거대한 규모의 네트워크를 형성할 수 있다. 결국 이러한 네트워크는 통제와 감시를 통한 안정적인 상태에 도달했을 때 그것은 전체 면역 시스템을 결정하게 된다.



(그림 2) 유전자 복제

3.2 면역학 기반의 IDS개발의 이점

인간 면역 체계의 복잡한 능력을 컴퓨터 위에서 구현할 수 있다면 면역 시스템의 세 가지 특징(분산화, 자가조직화, 경량화)에 근거하여 효율적(Efficiency), 강인성(Robustness), 확장성(Extensibility), 규모성(Scalability), Configuarablity, 적응성(Adaptability), 전역 분석능력(Global Analysis)을 가진 네트워크 침입탐지시스템을 개발할 수 있다.

첫째, 인간 면역 체계는 분산화 되어 있다. 인간 면역 체계는 서로 다른 다양한 종류의 세포들 간의 상호작용을 통하여 이뤄진다. 중앙 조정자(co-ordinator)를 두는 대신에 인간 면역 체계는 유전적 항체들을 이용한 항체 진압과 활동사이의 안정적인 상태를 유지함으로써 면역 반응의 적당

한 수준을 유지한다. 인간 면역 체계는 서로 다른 다양한 종류의 세포들 간의 상호작용을 통하여 이뤄진다. 중앙 조정자(co-ordinator)를 두는 대신에 인간 면역 체계는 유전적 항체들을 이용한 항체 진압과 활동사이의 안정적인 상태를 유지함으로써 면역 반응의 적당한 수준을 유지한다.

둘째, 면역 시스템은 자가 조직화(Self-Organization)가 가능하다. 전체 면역 반응은 다음의 세 가지 진화단계로 구성된다. 유전자 라이브러리(gene library) 진화는 효율적인 항체를 생산하며, 부정적 선택(negative selection)은 부적절한 항체를 죽인다. 마지막으로 유전자 복제(clonal selection)는 제대로 수행되고 있는 항체를 복제한다. 이러한 세 가지 단계들은 중앙 조직 혹은 미리 정의된 정보를 이용한 직접적인 수행보다 더 자가조직화 된다.

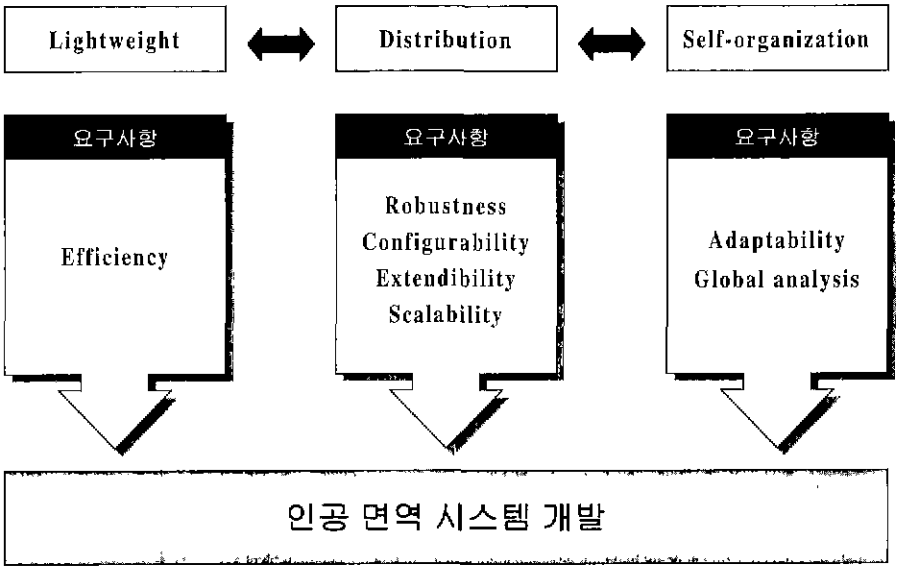
셋째, 면역시스템을 도입하면 경량화가 가능하다. 인간 면역 체계는 경량화되어 있다. 다음에 나오는 장치들은 경량화를 가능하게 하며 다음의 세 가지 아이디어에 중점을 두고 있다. i) 엄청난 수의 항원들이 적은 수의 항체들에게 어떻게 탐지될 것인가. ii) 이미 알려져 있는 항원 정보가 효율적으로 어떻게 재사용 되나. iii) 다양한 항체들이 유전자의 제한된 수만으로 어떻게 생산될 수 있나. 근접 바인딩(approximate binding)과 기억세포(memory cell) 그리고 유전자 표현(gene expression)이라는 메커니즘을 통해 면역시스템은 경량화를 가능케 한다.

3.3 경량화 메커니즘

근접 바인딩(Approximate Binding) : 면역 반응은 항체와 항원사이의 바인딩 유연이 큰 폭으로 상승하였을 때 활성화 된다. 다른 말로, 하나의 항체는 그들의 유연이 상승할 수 있을 만큼의 어떠한 항원 집단을 탐지할 수 있다. 이러한 근접 바인딩은 면역 체계의 보편성을 증가시키는 역할을 한다.

기억 세포(Memory Cells) : 메모리 세포는 기존에 탐지되었던 항원 에피토프들의 유전적 정보를 저장하며 그들이 미래에 전과 동일한 항원을 만났을 경우 신속하고 효율적으로 반응한다

유전자 표현(Gene expression) : 면역 체계는 항



(그림 3) 인체 면역 시스템의 도입과 기대 효과

원들의 광범위한 범위에 대해 효율적 탐지를 보장함으로써 항체 변화를 유지한다. 항체의 성장 과정에서 유전자 라이브러리로부터 다양한 항체들을 형성하기 위하여 유전자 표현과 같은 몇몇의 유전적 장치들을 탑재하고 있다. 이러한 장치들의 주 아이디어는 새로운 항체들의 거대한 수가 유전자 라이브러리에서 유전자 조각의 새로운 조합만으로 생산될 수 있게 하기 위해서이다

위에서 볼 수 있듯이 경량화(Lightweight), 분산화(Distribution), 자가조직화(Self-organization)는 인간의 면역체계를 구성하는 가장 기본적인 구조이다. 이러한 구조를 이용하여 아주 적은 양으로 쪼개져서 인체에 퍼진 항체(antibody)가 인체에 침투한 항원(antigen)을 탐지할 수 있는 것이다. 따라서 이러한 세 가지 면역 특성을 컴퓨터 작동원리로 사용한다면 기존의 외부침입 탐지 기술이 가지고 있는 문제점들을 해결할 수 있을 것으로 기대한다.

4. 인체 면역 기반의 침입 탐지 시스템 개발

인간의 면역 메커니즘을 컴퓨터 분야에 응용하려는 시도는 최근 미국의 University of New Mexico [15][16][17][18], Santa Fe Insitute, 영국의 UCL(런던대학) [5][6][7][8]등과 같은 소수의 기관에 의해서만 연구되고 있다. 국내에서는 상명대학[2][3][4]과 항공대학[1], 중앙대 등이 있다. New Mexico대학이나 Santa Fe Institute에서 이루어지고 있는 연구는 주로 면역시스템이 갖는 변화의 인식 메커니즘, 유전자 알고리즘의 면역학 적용, 인공생명과 유전자 알고리즘, 면역시스템의 기억 메커니즘 등이다. 한편 런던대학과 상명대학 연구팀의 접근방법은 면역메커니즘의 자기(Self)/비자기(Non-Self)의 구분, T-Cell과 B-Cell의 성장 소멸과정, 그리고 Cell들간의 상호작용 과정에 중점을 두어 이를 직접 시스템 개발에 응용하는데 초점이 맞추어져 있다.

아직도 면역 기반의 침입탐지 시스템 개발은 시작단계에 불과하다. 향후 더 많은 연구와 노력이 필요할 것으로 생각된다.

참고문헌

[1] 이종성, 채수환, "컴퓨터 면역 시스템을 기반으로 한 지능형 침입 탐지 시스템," 정보처리 논문지, 6권 12호, 3622-3633, 1999 12월.

[2] 정길호, 김정원, 최종욱, "인간 면역 체계와 네트워크 침입 탐지", 99 춘계공동학술대회 논문집, 한국지능정보시스템학회, 한양대학교 1999. 6. 4.

[3] 정길호, 김정원, 최종욱, "인공면역 모델을 이용한 네트워크 침입 탐지", 99 춘계공동학술대회 논문집, 한국지능정보시스템학회, 한양대학교 1999. 6. 4.

[4] 김회준, 최종욱, "에이전트 기반의 침입탐지 시스템 구현," 통신정보 보호학회지, 9권 3호, pp.83-96, 1999, 9.

[5] J. W. Kim, and P. J. Bentley (1999). "Negative Selection and Niching by an Artificial Immune System for Network Intrusion Detection" A late-breaking paper submitted to Genetic and Evolutionary Computation Conference (GECCO '99), Orlando, Florida, July 13-17.

[6] J. W. Kim, and P. J. Bentley (1999), "The Human Immune System and Network Intrusion Detection", 7th European Congress on Intelligent Techniques and SoftComputing (EUFIT '99), Aachen, Germany, September 13- 19.

[7] J. W. Kim, and P. J. Bentley (1999), "The Artificial Immune Model for Network Intrusion

Detection", 7th European Congress on Intelligent Techniques and Soft Computing (EUFIT'99), Aachen, Germany, September 13- 19.

[8] J. W. Kim (1999), "The Artificial Immune System for Network Intrusion Detection", Phd Student Workshop, Genetic and Evolutionary Computation Conference, Orlando, Florida. July 13-17 (GECCO-99).

[9] K. L. Fox, R. R. Henning, J. H. Reed, and R. P. Simonian, A Neural Network Approach Towards Intrusion Detection, Technical Report, Government Info. Systems Division, Harris Corp., July 1990.

[10] J. Frank, "Artificial Intelligence and Intrusion Detection: Current and Future Directions", NSA URP MDA904-93-C-4085, June, 1994.

[11] D. Goldberg. Genetic Algorithm in Search, Optimization and Machine Learning. Addision-Wesley, 1989.

[12] R. Heady, G. Luger, A. Maccabe, and M. Servilla, The architecture of a network level intrusion detection system, Technical Report, Department of Computer Science, University of New Mexico, August 1990.

[13] J. O. Kephart, A Biologically Inspired Immune System for Computers, High Integrity Computing Laboratory, IBM Thomas J. Watson Research Center, MIT Press, 1994.

[14] S. Kumar, G. and Spafford, "A Pattern Matching model for Misuse Intrusion Detection". In Proceedings of the 17th National Computer Secutiry Conference, October 1994

[15] S. Forrest, S. A. Hofmeyr, A. Somayaji, and T. A. Longstaff, "A sense of self for Unix processes," *In Proceedings of 1996 IEEE Symposium on Computer Security and Privacy* (1996).

[16] S. A. Hofmeyr, A. Somayaji, and S. Forrest, "Intrusion Detection using Sequences of System Calls," in *the Journal of Computer Security*, Vol. 6 (1998) pg 151-180 .

[17] C. Warrender, S. Forrest, B. Pearlmutter, "Detecting Intrusions Using System Calls: Alternative Data Models," Proceeings of 1999 IEEE Symposium on Security and Privacy pp. 133-145 (1999).

[18] P. D'haeseleer, S. Forrest, and P. Helman, "An immunological approach to change detection: algorithms, analysis, and implications", In *Proceedings of the 1996 IEEE Symposium on Computer Security and Privacy* (1996).

[19] R. Graham, FAQ: Network Intrusion Detection Systems, http://www.robertgraham.com/pubs.

최 종 욱

1982년 아주대학교 공대 산업공학과 산업공학 학사
서울대 대학원 경영학과 경영학과 (석사과정)
1988년 University of South Carolina 정보학박사
1985-1986년 Institute of Information Management, Technology and Policy at University of South Carolina Research Assistant('C' Programmer)
1986-1987년 Johnson C. Smith University(Charlotte, NC) Computer System Specialist
1988-1997년 한국과학기술원(KIST) 시스템 공학센터 인공지능연구부 지식처리 연구실 실장
1991년-현재 상명대학교 정보통신학부 정보과학과 부교수
관심분야 : 워터마킹, 지능형 교통 시스템, 영상인식기술, 네트워크 시스템, 보안 기술