퍼지 및 지능시스템학회 논문지 2003, Vol. 13, No. 2, pp. 169-174

인공 면역계를 기반으로 하는 적응형 침입탐지 알고리즘

Adaptive Intrusion Detection Algorithm based on Artificial Immune System

심귀보 · 양재원

Kwee-Bo Sim and Jae-Won Yang

중앙대학교 전자전기공학부

요 약

인터넷 보급의 확산과 전자상거래의 활성화 그리고 유·무선 인터넷의 보급에 따른 악의적인 사이버 공격의 시도가 점점 증가하고 있다. 이로 인해 점차 더 많은 문제가 야기될 것으로 예상된다. 현재 일반적인 인터넷상의 시스템은 악의적인 공격에 적절하게 대응해오지 못하고 있으며, 다른 범용의 시스템들도 기존의 백신 프로그램에 의존하며 그 공격에 대응해오고 있다. 따라서 새로운 침입에 대하여는 대처하기 힘든 단점을 가지고 있다. 본 논문에서는 생체 자율분산시스템의 일부분인 T세포의 positive selection과 negative selection을 이용한 자기/비자기 인식 알고리즘을 제안한다. 제안한 알고리즘은 네트워크 환경에서 침입탐지 시스템에 적용하여 기존에 알려진 침입뿐만 아니라 새로운 침입에 대해서도 대처할 수 있다.

Abstract

The trial and success of malicious cyber attacks has been increased rapidly with spreading of Internet and the activation of a internet shopping mall and the supply of an online, or an offline internet, so it is expected to make a problem more and more. The goal of intrusion detection is to identify unauthorized use, misuse, and abuse of computer systems by both system insiders and external penetrators in real time. In fact, the general security system based on Internet couldn't cope with the attack properly, if ever, other regular systems have depended on common vaccine softwares to cope with the attack. But in this paper, we will use the positive selection and negative selection mechanism of T-cell, which is the biologically distributed autonomous system, to develop the self/nonself recognition algorithm and AIS (Artificial Immune System) that is easy to be concrete on the artificial system. For making it come true, we will apply AIS to the network environment, which is a computer security system.

Key words : positive selection, negative selection, positive detector, negative detector, hybrid detector

1. 서 론

네트워크 공격기법이 전통적인 공격모델에서 새로운 기법으로의 변화는 보안 시스템이 보편화되면서 이를 극복하고자 하는 침입자들의 노력에서 시작된다. 현재의 보안모델에서는 일반적으로 침입자가 우세하며 방어자는 기존의 공격방법에만 대응하는 방식의 주기를 가진다. 또한 인터넷이 일상의 중요한 일부가 되면서 사이버테러, 사이버범죄가 구체화, 조직화 되는 것도 전통적인 공격모델의 변화에 큰 영향을 주고 있다. 전통적인 공격기법 변화의 주된 원동력은 방어자의 보안수준 향상이다. 방화벽과 침입탐지시스템의 보편화는 전통적인 공격기법에 효과적인 대응수단을 제공한다. 하지만 이러한 방어벽을 극복하고 성공적으로 시스템에 침입하기 위한 기술 및 도구들이 최근 몇 년간 지속적으로 개발되고 있다[2-5].

생물학적인 면역계에서 외부 항원의 침입을 탐지하는 역할을 수행하는 세포는 B세포이다. B세포 속에서 다른 세포들에서는 멀리 떨어져 있는 두 개의 유전자가 B세포에서는 가까이 존재하고 있다. 그것은 다름 아닌 항체분자를 만들도록 명령하는 유전자였다. 항체분자는 면역글로불린이라는 단백질에 속하며 H사슬(Heavy chain)과 L사슬(Light chain)이라 부르는 두 개의 폴리펩티드 사슬로 이루어져 있다. 그런데 두 가지 폴리펩티드를 만드는 유전자들이 B 세포 속에서 서로를 향하여 이동한다. 이 발견이 실마리가 되어 항체를 만드는 유전자가 달리 예를 찾아볼 수 없으리만큼 교묘한 방식으로 다양한 항원에 대응할 수 있는 항체분자의 구조를 만든다는 사실이 밝혀졌다. 적은 수의 항체로써 다양한 항원에 대하여 침입을 탐지하는 것이 가능한 것은 다름 아닌 서로 다른 유전자 단편의 결합(재구성)이다[1]. 하지만 현재 이러한 면역계의 항체 구성원리를 모델링한 알고리즘으로는 미국의 포레스트 등이 생체 면역계의 면역세포 생성원리를 모델링하여 구성한 negative detector를 이용하여 변이된 네트워크 공격의 침입을 탐지하는 알고리즘이다[5]. 그러나 포레스트 등의 알고리즘도 면역계의 B세포를 이용하는 침입탐지

접수일자 : 2002년 11월 9일
완료일자 : 2003년 3월 15일
본 연구는 서울시·중소기업청의 연구비지원에 의한 2002년도 중앙대학교 산학연컨소시엄사업에 의해 수행되었습니다. 연구비지원에 감사드립니다.

방식과는 달리 T세포의 역할을 모델링한 알고리즘으로 본 논문에서도 생체 면역계의 T 세포의 생성원리를 이용한 positive selection과 negative selection을 모델링 하고 SYN flooding attack에 대처하는 알고리즘을 제안한다. 즉, T 세포가 생성되기 위해서 통과해야 하는 두 가지 selection 과정을 모델링하여 생성된 디텍터를 이용하여 새로이 입력되는 데이터에 대해 자기와 비자기 여부를 검사하는 알고리즘이다.

2장에서는 생체 면역계에서 성숙한 면역세포의 생성과정과 그들의 생성원리를 설명할 것이다. 3장에서는 positive selection을 이용한 SYN flooding attack의 대처방법을 알아보고, 4장에서는 negative selection을 이용한 대처방법을 제안한다. 그리고 5장에서는 positive selection과 negative selection을 혼용한 침입 탐지 알고리즘을 제안한다.

2. 생체면역계의 면역세포 생성원리

2.1 BIS(Biological Immune System)

생명체의 방어체계인 면역계는 박테리아, 기생균, 병원균, 독소, 바이러스 등과 같이 항원이라고 통칭하는 매우 다양한 외부유기체나 단백질에 대하여 생명체의 세포와 장기를 방어할 수 있는 매우 정교하고 복잡한 시스템이며 개체를 건전한 상태로 유지시키기 위해 반드시 필요한 기능이다. 또한 면역계는 virus 감염과 종양발생에 의해 변이한 자기세포를 배제하는 작용도 가지고 있다. 이러한 생명체의 면역계는 중앙처리 장치인 뇌의 명령에 따르는 것이 아닌 각 요소의 자율적인 행동이 유기적으로 결합되어 형성된 자율분산시스템으로 항원을 인식하는 기능, 정보처리 기능, 학습 및 기억능력, 자기와 비자기의 구별능력, 분산시스템으로서 전체의 조화를 유지하는 능력 등을 가지고 있다.

2.2 면역세포 형성 원리

BIS에서 가장 중요한 역할을 하는 면역 세포가 외부에서 침입한 항원을 제거하는 면역 반응을 정상적으로 수행하기 위해서 각각의 면역 세포들은 2가지의 요소에 의존하게 된다. 하나는 각각의 세포사이의 협력과 공조이다. 또 다른 하나는 항원의 인지 능력과 구별 능력이다. 면역 세포의 항원을 인지하는 능력은 자기 세포와구별되는 항원을 구별하고 이의 항원결정소의 특성을 가지고 있는 면역 세포를 통해 항원을 제거하는 면역 반응을 일으키는 가장 중요한 능력인 것이다.

면역 세포가 자기 세포를 인지하는 방법으로는 MHC 단백질을 이용한다. 개체에는 각각 개인적인 특징을 이루는 단백질이 존재하며, 단백질을 생성하는 유전자들을 주조직 적합성 복합체(major histocompatibility complex, MHC)라 하며, 이렇게 생성된 단백질을 MHC 단백질이라고 한다. 이 MHC 단백질을 인식하는 부분이 면역세포에 존재하며 이를 이용해 자신의 세포인지를 판단하게 된다. B세포나 T세포와 같이 특정 항원에 대해 적용되는 면역 세포는 생성될 때 다양한 항원들의 특성에 부합되는 부분이 존재하며 이를 항원수용체(Antigen Receptor)라 한다. 항원수용체는 면역 세포가 생성될 때 유전자의 돌연변이 및 교차를 이용하여 다양성을 내포하며 생성된다.

자기를 판별해주는 MHC 단백질을 인식하는 부분과 항원의 종류를 판별하는 항원수용체의 특성을 지니는 대표적인 면역 세포는 세포독성 T세포이다. 세포독성 T세포는 항원에 감염된 자기 세포를 제거하는 역할로 먼저 자기 세포인지를 판별하고 자기 세포에 항원이 존재하는 가를 검사하므로 이 두 가지의 인식부를 모두 가지고 있다. 이러한 T세포의 인식부를 T세포 수용체(T-cell receptor)라고 한다. T세포 수용체가 면역계에서 정상적으로 동작되지 않으면 자기 세포를항원으로 인식하게 되어 공격하게 된다. 따라서 면역계는 면역세포 초기 생성시 MHC 인식부와 항원수용체의 정상적인 동작여부를 확인하면서 면역 세포를 생성하여 면역계를 구성한다. 수용체의 정상적인 동작여부를 가리는 방법으로 사용되는 것이 Positive Selection과 Negative Selection이다.

Negative Selection은 항원의 인식에 있어서 자기를 항원으로 인식하는 것을 배제하기 위한 방법이다. 항원수용체가 MHC 단백질을 항원으로 인식하면 모든 자기 세포를 항원으로 인식하게 된다. 때문에 항원으로 MHC 단백질을 인식하지 못하게 하기 위해 면역세포에 MHC 단백질을 결합시켰을 때 항원수용체가 부정적인 선택을 하는 세포만으로 구성된다. 이때 긍정적인 선택을 하는 면역세포는 MHC 단백질을 항원으로 인식하는 세포들이므로 죽이거나 다시 항원 수용체를 형성하는 단계를 거치게 된다.

Positive Selection은 각 면역세포의 MHC 인식기능을 확인하는 선택 방법이다. 자기세포에서 분비되는 MHC 단백질을 정확히 인지할 수 있는 면역세포만이 사용가능하기 때문에 갓 생성된 면역세포에 MHC 단백질을 결합시켜 긍정적인 선택이 되는 세포들로만 면역 세포를 구성하게 되며 선택되지 않은 면역 세포들은 자기 세포를 인지하지 못하는 것이므로 제거 또는 재배열 등의 방법을 사용하여 면역계를 유지한다. 다음 3장에서 SYN Flooding Attack 탐지를 위해서 쓰인다.

이 두 가지 선택을 거친 면역세포는 MHC 단백질을 자신으로 인식하면서 이를 항원으로 인식하지 못하게 구성되어 생명체에서 정상적인 면역반응을 형성한다. 그림 1은 생체 면역계에서 정상적인 면역 세포의 형성과정을 보여주고 있다.

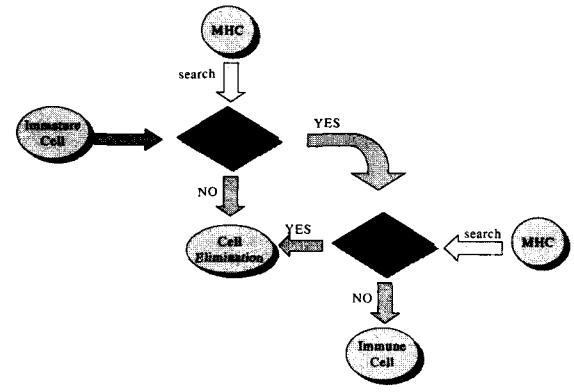

그림 1. 면역 세포의 형성과정
Fig. 1. The formation procedure of Immune cells

3. Positive Selection 알고리즘에 의한 SYN Flooding Attack의 적용

3.1 TCP SYN Flooding Attack

클라이언트 시스템이 서버 시스템이 제공하는 서비스를 이용하고자 TCP 연결을 신청할 때, 클라이언트와 서버는 일련의 메시지를 교환하게 된다. 클라이언트는 서버에 SYNx 메시지를 보냄으로써 연결을 신청하며 그때, 서버는 SYNy와 ACKx+1 메시지를 클라이언트에게 보냄으로써 SYNx 메시지 수신을 확인한다. 여기서 클라이언트가 ACKy+1 메시지를 서버에게 보내게 되면 신청하였던 TCP 연결은 이루어지게 되는데, 그림 2의 3-way handshake가 그것이다. 하지만, 클라이언트가 ACKy+1 메시지를 보내지 않게 되면 서버는 그 메시지가 올 때까지 일정시간 동안 기다리게 되는 "Half-Open State"가 되는 것이다. 시스템의 운영체제마다 각각의 backlog queue의 용량은 다르지만 SYN flooding attack이 급격하게 이루어지게 되면 그 queue는 가득 차게 되어 서버의 서비스가 중지가 되는 공격형태이다.

본 논문에서는 TCP 연결을 신청하는 패킷이 서버에 유입될 때 이 패킷의 의도를 판단할 방법으로 게이트웨이와 라우터를 경유하여 유입되는 패킷을 모니터링 하여 그 패킷을 캡쳐, 분석하여 침입여부를 판단하는 패킷 모니터링 방식을 모델링 한다[2-3].

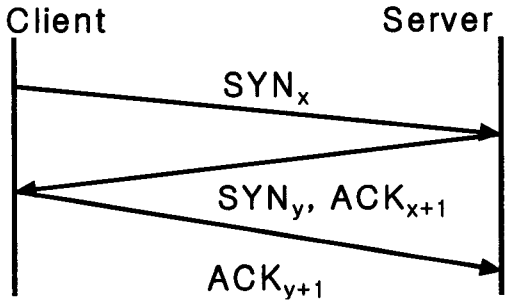

그림 2. 3 way-handshake
Fig. 2. 3 way-handshake

3.2 SYN Flooding Attack에 대한 Positive Selection 알고리즘.

위에 제시된 packet monitoring을 이용하여 캡쳐 및 분석된 패킷에서 MHC 단백질로 삼는 데이터는 정상적인 패킷의 SYN과 RST, 그리고 sequence number이다[1]. 이때 새로이 유입되는 패킷에서 RST 값과 SYN 값, 그리고 sequence number 값에 해당하는 bit 들을 Positive Detector와 매칭 후 일치하는 데이터는 positive detector를 구성하는데 사용하고, 일치하지 않는 데이터는 알고리즘에 제시된 방법으로 처리한다.

이에 대한 알고리즘은 다음과 같으며 그림 3은 알고리즘의 개념도이다.

Step 1. 패킷을 Capture한다.
Step 2. 패킷을 분석한다.
Step 3. 정상적인 패킷에서 추출된 데이터를 이용하여 self string set을 설정한다.
Step 4. Self string set을 바탕으로 positive detector를 초기화 한다[4-5].
Step 5. 새로이 유입되는 패킷을 분석한 후 positive detector와 matching 후 일치하는 경우에는 연결 신청을 받아들이고, 그렇지 않을 경우에는 현재의 세션을 중지 시켜서 SYN Flooding Attack에 대처한다[6].

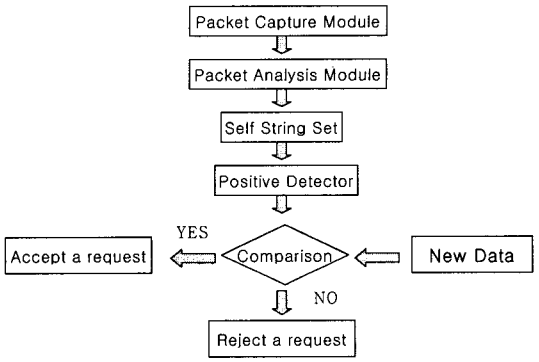

그림 3. Positive Detection 알고리즘 개념도
Fig. 3. The flowchart of Positive Detection Algorithm

3.3 Simulation

그림 4는 self set의 구성을 보여준다. A, C, D 성분들은 BIS의 MHC 단백질의 역할을 한다. 그들은 새로운 패킷에 위치하게 된다. 각 구성 요소들의 내용은 다음과 같다.

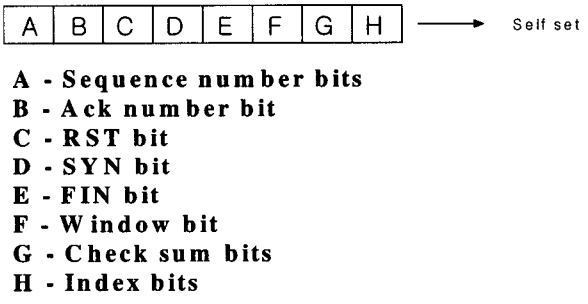

그림 4. 자기 테스트를 위한 스트링 구성
Fig. 4. Construction of string for self testing

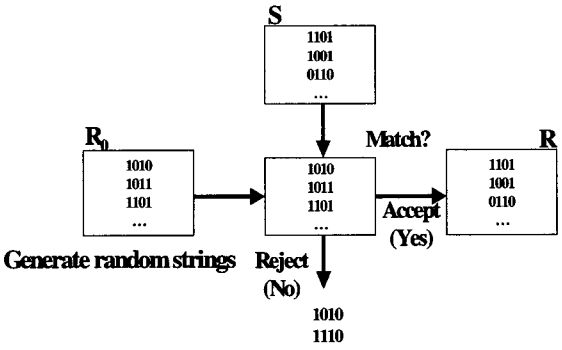

그림 5. Positive Detector 생성
Fig. 5. The composition of Positive Detectors (PD)

Positive Detector (PD, R)는 self string 에서 랜덤하게 생성된 데이터 (R_0)와 매칭 된 데이터로 이루어진 detector

집합이다. 이후 R_0와 매칭 후 Self라고 판단된 R0에 해당하는 string은 R에 추가된다. 그림 5의 과정을 거친 PD는 시뮬레이션 초기에 50개로 그 수를 제한하며, 이에 매칭되게 될 데이터 또한 50개로 제한한다. 즉, 50개의 PD를 통해 탐지해야 할 침입 시도의 수가 50번이 되는 것이다. 50번의 침입 시도에 대해서 얼마만큼의 탐지 횟수를 보이는지는 결과는 실험결과 테이블 1에 보여 진다. 또한 Non_Self를 1,000회로 한정한 후 각각의 detector를 변화시키면서 침입을 탐지한 결과는 테이블 2에 보여 진다.

4. Negative Selection 알고리즘

흉선에서 T세포를 생성하는 것과 유사하게, detector 스트링들은 랜덤하게 생성될 수 있다. 보호되어야 할 self 스트링들과 매칭 되는 것들은 제거 된다. 어떤 self 스트링들과 매칭 되는데 실패한 것들로만 detector 집합, R을 구성한다. 이때 사용되는 선택 방법이 negative selection이다. 이 과정은 요구되는 방어 수준에 이를 때까지 계속된다.

그 과정은 우선 랜덤하게 생성된 스트링, R_0 를 이미 설정해 두었던 self 스트링, S와 매칭을 시킨다. 이때 self 스트링과 패턴이 같다고 판단되었을 경우에는 reject시키고 그렇지 않고 새로운 패턴일 경우에만 accept를 시킨 후, 기존의 detector, R을 갱신하는 데 사용된다. 그림 6에서, negative selection을 이용하여 S와 다른 스트링을 detector 집합으로 설정하게 되는 것이다. 이는 특정 징후에 의해 선택하는 positive selection과는 다르게 변이된 스트링에 대해서 탐지를 하기 위한 방식이다. negative selection을 이용하는 알고리즘은 그 생성과정이 positive selection의 방식 중 선택방법이 반전된 알고리즘이다. 즉, self data와 매칭 되지 않은 데이터 집합으로 negative detector (ND)를 구성하여 침입의 시도를 탐지하는 것이다. 그림 7에서는 이미 구성된 ND를 이용하여 침입을 탐지하는 flowchart이다.

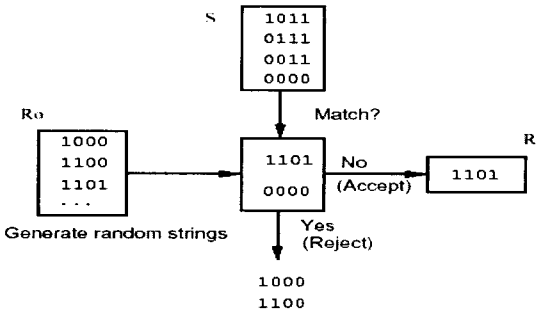

그림 6. Negative Detector의 구성
Fig. 6 Constructing a set of detectors R from S

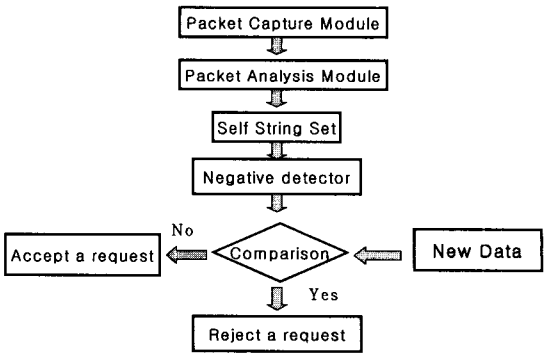

그림 7. Negative Detection 알고리즘 개념도
Fig. 7 The flowchart of Negative Detection Algorithm

테이블 1과 2는 그 시뮬레이션 결과를 나타낸다. 테이블 1에서는 detector의 개수가 50개이며 침입시도도 50회로 제한하였다. 하지만 테이블 2에서는 침입시도의 횟수를 1,000회로 한정하였으며, 이에 detector의 개수를 변화시키면서 침입을 탐지한 결과를 보여준다. 한편, negative detector를 이용하는 침입탐지는 향후 변이된 침입에 대해 방편이 될 것이다 [5][7-8].

5. Positive selection과 Negative selection의 혼용 알고리즘

침입탐지 시스템은 분석 대상에서 추출한 정보를 이용해서 침입 여부를 판단하는데, 탐지 방식에 따라 오용탐지(misuse detection)방식과 비정상행위 탐지 (anomaly detection)방식으로 나눌 수 있다. 오용탐지 방식은 알려져 있는 공격 행위로부터 특정 signature를 추출해내고, 분석 대상에 그런 signature가 존재하는지를 확인하여, 존재할 경우 침입임을 판단하는 방식이다. 그렇기 때문에 알려져 있는 공격에 대한signature 목록을 유지해야 하고, 이 목록을 얼마나 최신의 버전으로 유지하느냐에 따라 새로 나온 공격의 탐지율이 달라진다. 이때 사용되는 선택방식이 positive selection이다. 오용탐지방식은 비정상행위 탐지 방식에 비해 상대적으로 False Positive율은 낮지만, signature 목록에 없는 공격을 탐지하지 못하는 False Negative율은 높다. 본 논문 3장에서 제안된 알고리즘은 일종의 오용탐지 방식으로써, 캡쳐된 packet을 분석, 파싱하여 추출된 데이터를 근거로 SYN, RST, Sequence number 비트들을 특정 signature로 활용하는 탐지 방식이라 할 수 있다.

이에 반해 비정상행위 탐지 방식은 기존의 네트워크 사용 상황을 기반으로 정상적인 행위의 범위를 정의해두고, 이러한 정상적인 행위에 어긋나는 모든 행위를 비정상행위로 규정하고 탐지한다. 비정상행위 탐지 방식은 정상적인 행위의 범위를 정의하는 것이 가장 중요하면서도 모호한데, 가장 쉽게 접근할 수 있는 방법이 통계적인 방법에 기반 하는 것이다. 일정 시간 네트워크 상황을 모니터링 하면서 모니터링 하는 네트워크의 사용상황을 통계적으로 분석하여 그러한 통계에 비해 비정상적인 상황이 나타날 경우를 탐지하는 방식이다.

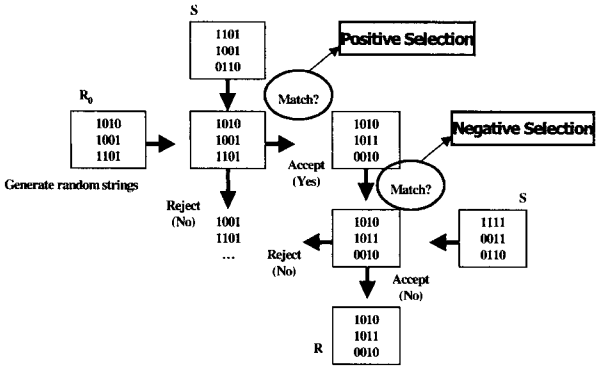

그림 8. Hybrid Detector의 생성과정
Fig. 8 Composition procedure of Hybrid Detector(HD)

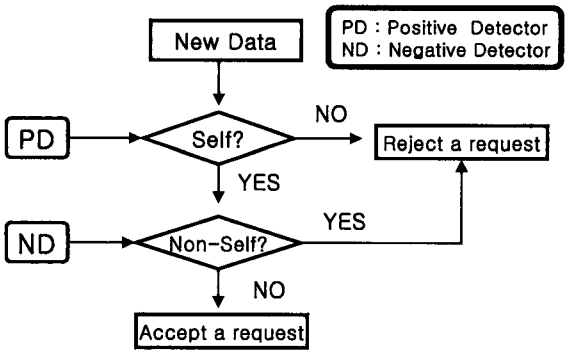

그림 9. 혼용 알고리즘의 개략도
Fig. 9. The flowchart of Hybrid Detection algorithm

본 논문에서는 언급한 두 가지 방식을 혼용하기 위해 그림 8 (Case_1)과 9 (Case_2)의 두 알고리즘을 제안한다. 그림 8의 알고리즘에 의하면 유입되는 데이터가 Non_Self라는 확실한 근거와 기준을 서술할 수 있을 경우 사용되는 것으로써 하나의 detector를 구성하여 Non_Self의 유입을 탐지하게 된다. 이에 반하여, 그림 9의 알고리즘에 의하면, 새로운 데이터가 유입될 때, PD와 매칭을 한 후 그 결과에 따라 각각의 다음 과정으로 진행되게 된다. 첫 번째 탐지를 거쳐서 긍정의 결과를 나타낸 데이터만 두 번째 탐지를 ND에 의해서 행해지게 된다. 그림 8의 과정에서는 다른 detector의 개수와 동일한 HD의 개수를 산정하여 침입을 탐지하였으며, 그림 9의 과정에서는 PD의 개수와 ND의 개수를 동일하게 반씩 생성하여 침입의 시도, 1,000회를 탐지하게 시뮬레이션 하였다.

6. 실 험 결 과

시뮬레이션은 Non_Self의 개수는 1000개이며 이를 탐지하기 위해서 Table 1의 경우는 detector의 개수가 100개에서 800개까지 변화하였으며, Table 2의 경우는 1000개의 Non_Self에 대해서 50개에서 900개까지 변화시켰다. 각각의 탐지 결과는 Table 1과 Table 2에 나와 있다.

주어진 Table의 결과로서 알 수 있듯이, Non_Self를 서술할 수 있으며 Self와 확연한 차이를 지닌 공격에 대해서는 그림 8의 경우처럼 하나의 HD를 구성하여 침입을 탐지한 결과, 테이블 1의 결과와 같이 다른 detector들 보다 detector의 개수와 독립적인 탐지를 하는 효율성을 보여 주었으며, 이에 반하여 Non_Self를 서술할 수 없는 변이적인 공격에 대해서는 그림 9에 표현되었듯이, PD와 ND를 이용하여 침입을 탐지한 결과는 테이블 2의 결과와 같이, 변종된 공격에 대한 ND의 침입 탐지율이 상대적으로 저조함을 보여준다.

Table 1. Case 1의 결과 테이블
Table 1. The result of Case 1

# of detector \ Type	Positive Detection	Negative Detection	Hybrid Detection
100	936.30	62.88	890.01
200	936.58	62.72	890.03
400	936.90	62.56	890.04
600	937.06	62.40	890.06
800	937.12	62.20	890.06

Table 2. Case 2의 결과 테이블
Table 2. The result of Case 2

# of detector \ Type	Positive Detection	Negative Detection	Hybrid Detection
50	936.04	62.95	48.0
100	936.2	62.98	96.1
150	936.28	62.82	144.98
200	936.36	62.88	193.02
300	936.56	62.42	290.0
600	936.92	62.42	580.74
900	936.9	62.18	871.48

하지만 PD와 ND를 이용하여 침입을 탐지하였던 혼용 탐지의 결과가 단독적인 PD를 이용한 경우보다 다소 저조하지만 변종된 공격의 탐지를 위한 ND보다는 훨씬 효율적인 것을 보여주고 있다. 이는 알려진 공격과 변종된 공격을 동시에 탐지한다는 차원에서 탐지의 신뢰도 향상에 혼용 알고리즘의 유효성을 확인할 수 있었다.

7. 결 론

생체의 면역계는 구조적으로 자율 분산 시스템이다. 특히 독립적으로 구성된 각각의 세포들은 유기적으로 상호 통신과 협조를 통해 외부에서 침입한 병균 및 이물질에 대해 방어를 하며, 이후 변이된 것에 대해서도 학습과 기억 세포를 통해 2차 방어를 하고 있다. 이에 본 논문에서는 생체 면역계의 면역 세포를 모델링 함으로써 컴퓨터 환경에서 발생된 바이러스 및 침입시도에 대해서 대처하는 알고리즘을 제안하였다. T세포의 생성과정 즉, positive selection과 negative selection을 이용한 알고리즘은 정상적인 접근에 대한 인식과정과 비정상적인 침입에 대한 이중적인 인식과정을 거치기 때문에 침입 탐지의 신뢰도를 향상시킨다. 다만 비정상적인 침입에 대한 ND의 탐지율이 저조한 것은 ND의 다양성이 확보되지 못한 것에서 연유되기에 ND의 다양성을 구현하는 것이 향후 과제이다.

참 고 문 헌

[1] 타다 토미오 지음 황상익 옮김, 면역 의미론, "자기(自己)란 무엇인가", 한울 과학문고, pp. 53, 1998.

[2] Computer Emergency Response Team, "TCP SYN Flooding and IP Spoofing Attacks", *CERT Advisory: CA*, pp. 96-21, 1996.

[3] S.Y. Lee and Y.S. Kim, "A RTSD Mechanism for Detection of DoS Attack on TCP Network," Proceedings of KFIS 2002 Spring Conference, pp. 252-255, 2002.

[4] P.D' haeseleer, S, Forrest, and P. Helman. "An immunological approach to change detection: Algorithms, analysis and implication," *Proceeding of the 1996 IEEE Symposium on Research in Security and Privacy,* Los Alami. 1996.

[5] A. Somayaji, S. Hofmeyr, and S. Forrest, "Principles of a Computer Immune System," *New Security Paradigms Workshop*, pp. 75-82, 1998.

[6] W. Stevens, *TCP/IP Illustrated*, vol. 1, Addison Wesley Publishing, Company, 1994.

[7] J. B. Gu, D. W. Lee, K. B. Sim, and S. H. Park, "An Immunity-based Security Layer against Internet Antigens," *Transactions on IEICE*, vol. E83-B, no.11, pp. 2570-2575, 2000.

[8] D. Dasgupta, and S. Forrest, " An Anomaly Detection Algorithm Inspired by the Immune Systems and Their Applications," *Springer*, pp. 262-276, 1999.

저 자 소 개

심귀보(Kwee-Bo Sim)

1984년 : 중앙대학교 전자공학과 공학사
1986년 : 동 대학원 전자공학과 공학석사
1990년 : The University of Tokyo 전자공학과 공학박사
2001년~2002 : 대한전기학회 제어및시스템 부문회 학술이사
2003년~현재 : 한국퍼지 및 지능시스템학회 부회장
2000년~현재 : 제어자동화시스템공학회 이사
2003년~현재 : 일본계측자동제어학회(SICE) 이사
1991년~현재 : 중앙대학교 전자전기공학부 교수

관심분야 : 인공생명, 진화연산, 지능로봇시스템, 뉴로-퍼지 및 소프트 컴퓨팅, 자율분산시스템, 로봇비전, 진화하드웨어, 인공면역계 등

Phone : +82-2-820-5319
Fax : +82-2-817-0553
E-mail : kbsim@cau.ac.kr

양재원(Jae-Won Yang)

2002년 : 중앙대학교 전기전자공학부 공학사
2002년 9월~현재 : 동 대학원 전기전자공학부 석사 과정

관심분야 : 인공면역계, 진화연산, 인공생명, 네트워크 등

Phone : +82-2-820-5319
Fax : +82-2-817-0553
E-mail : emfvnf@jupiter.cie.cau.ac.kr