한국 퍼지 및 지능시스템 학회 2002, Vol. 12, No. 5, pp. 411-416

생체 면역계를 이용한 네트워크 침입탐지 시스템

Intrusion Detection System of Network Based on Biological Immune System

심귀보* · 양재원* · 이동욱* · 서동일** · 최양서**

Kwee-Bo Sim*, Jae-Won Yang*, Dong-Wook Lee*, Dong-Il Seo**, and Yang-Seo Choi**

* 중앙대학교 전자전기공학부

** 한국전자통신연구원 사이버테러기술 분석팀

요 약

최근 인터넷의 확산과 전자상거래의 활성화 그리고, 유·무선 인터넷의 보급과 더불어 악의적인 사이버 공격의 시도와 성공이 급속하게 증가하고 있다. 이것은 점차 더 많은 문제를 야기할 것으로 예상된다. 현재 일반적인 인터넷상의 시스템은 악의적인 공격에 적절하게 대응하지 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

Recently, 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 internet, so it is expected to make a problem more and more. Currently, the general security system based on Internet couldn't cope with the attack properly, if ever, other regular systems have depended on common softwares to cope with the attack. In this paper, we propose the positive selection mechanism and negative selection mechanism of T-cell, which is the biological distributed autonomous system, to develop the self/non-self recognition algorithm, the anomalous behavior detection algorithm, and AIS (Artificial Immune System) that is easy to be concrete on the artificial system. The proposed algorithm can cope with new intrusion as well as existing one to intrusion detection system in the network environment.

Key Words : 생체면역계(BIS), positive selection, negative selection, intrusion detection

1. 서 론

네트워크의 기술발전으로 인하여 사회 전반에 걸쳐 인터넷의 활용의존성이 매우 높아지고 있다. 이러한 네트워크 기술 발전의 반대급부로 악의적 목적을 둔 침입을 위한 서비스 거부 공격이 심각한 문제로 대두되고 있다. 여기서 서비스 거부 공격이란 일반적으로 시스템의 자원을 고갈 또는 마비시켜 서비스지원을 하지 못하게 하는 침입시도라고 볼 수 있다. 이들 중 가장 대표적인 서비스 거부공격으로는 일명 SYN Flooding 이라 불리는 공격형태가 있다[1]. SYN Flooding Attack은 인터넷환경에서 가장 많이 사용되어지는 TCP 기반의 프로토콜인 HTTP 와 FTP 서비스를 지원하는 시스템에 크게 영향을 미치게 된다. 이 공격은 TCP 프로토콜의 구조적 약점을 이용하는데 이를 해결하기 위해서는 프로토콜의 수정이외에는 사실상 정확한 해답이 없다.

서비스 거부 공격은 크게 주요 파일을 훼손시켜 목적 시스템의 동작을 방해하는 우회적 서비스 거부 공격과 목적 시스템의 자원 및 네트워크 데이터 전송을 위한 흐름제어 자원을 고갈시키는 공격으로 나눌 수 있다[2]. 현재 이를 해결하기 위한 여러 대안이 많이 연구되어 지고 있다.

본 연구에서는 생체 면역계의 T 세포의 생성원리를 이용한 positive selection과 negative selection을 모델링 하고 SYN flooding attack에 대처하는 알고리즘을 제안한다. 2장에서는 본 연구의 기본 배경인 생물학적 면역계(BIS: Biological Immune System)의 생성원리에 대해서 알아본다. 3장에서는 positive selection을 이용한 SYN flooding attack의 대처방법을 알아보고, 4장에서는 negative selection을 이용한 대처방법을 제안한다. 마지막으로 5장에서는 positive selection과 negative selection을 혼용한 침입탐지 알고리즘을 제안한다.

접수일자 : 2002년 7월 1일
완료일자 : 2002년 9월 30일
본 연구는 한국전자통신연구원의 인공면역 기반 차세대 인터넷 보안기술 개발의 용역으로 수행되었습니다. 연구비 지원에 감사드립니다.

2. 생체 면역시스템

2.1 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 시스템이다. 이것은 개체를 건전한 상태로 유지시키기 위해 반드시 필요한 기능이다. 또한 면역계는 바이러스 감염과 종양발생에 의해 변이한 자기세포를 배제하는 작용도 가지고 있다. 이러한 생체의 면역계는 중앙 처리 장치인 뇌의 명령에 따르는 것이 아닌 각 요소의 자율적인 행동이 유기적으로 결합되어 형성된 자율분산 시스템으로 동작하고 있으며 또한 항원을 인식하는 기능, 정보처리 기능, 학습 및 기억능력, 자기와 비자기의 구별능력, 분산시스템으로서 전체의 조화를 유지하는 능력 등을 가지고 있다.

2.1 면역세포 형성 원리

BIS에서 면역 세포들이 외부에서 침입한 항원을 제거하는 면역 반응을 정상적으로 수행하기 위해서 2가지의 요소에 의존한다. 하나는 각각의 세포사이의 협력과 공조이고, 다른 하나는 항원의 인지 능력과 구별 능력이다. 면역 세포의 항원을 인지하는 능력은 자기 세포와 구별되는 항원을 구별하고 이의 항원결정소의 특성을 가지고 있는 면역 세포를 통해 항원을 제거하는 면역 반응을 일으키는 가장 중요한 능력이다.

면역 세포가 자기 세포를 인지하는 방법으로는 MHC 단백질을 이용한다. 개체에는 각각 개인적인 특징을 이루는 단백질이 존재하며, 단백질을 생성하는 유전자들을 주조직적합성복합체(Major Histocompatibility Complex, MHC)라 하며, 이렇게 생성된 단백질을 MHC 단백질이라고 한다[2]. 이 MHC 단백질을 인식하는 부분이 면역세포에 존재하며 이를 이용해 다른 세포가 자신 것인지 아닌지를 판단하게 된다. B세포나 T세포와 같이 특정 항원에 대해 적용되는 면역 세포는 생성될 때 다양한 항원들의 특성에 부합되는 부분이 존재하며 이를 항원 수용체 (Antigen Receptor)라 한다. 항원 수용체는 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 세포를 항원으로 인식하게 되어 공격하게 된다. 따라서 면역계는 면역 세포 초기 생성시 MHC 인식부와 항원 수용체의 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.

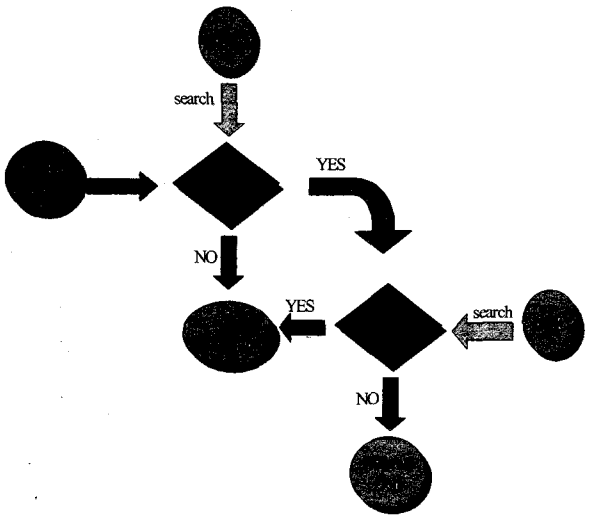


그림 1. 면역 세포의 형성과정
Fig 1. Formation process of immune cell in BIS

3. SYN Flooding Attack의 적용 알고리즘 : Positive selection 알고리즘

3.1 TCP SYN Flooding Attack

TCP SYN Flooding Attack은 앞에서 언급되었듯이 TCP의 약점인 신뢰성 지향적 연결을 이용하여 공격하는 침입시도의 일종이다. 그림 2와 같이 서버와 클라이언트 간에 연결요청을 할 경우에는 3way-handshake라는 정상적인 연결흐름이 이루어진다[4]. 하지만 클라이언트가 SYNx를 요청하고 서버로부터 SYNy와 ACKx+1을 받은 후 ACKy+1을 보내지 않으면 서버에서는 클라이언트로부터 응답이 올 것을 기대하고 반쯤 열린 "Half Open State" 가 된다. 물론 얼마간 다음 요청이 오지 않으면 해당 연결을 reset하게 된다. 이때 reset되기 전까지 메모리에는 backlog queue가 계속 쌓이게 되는데 이러한 reset이 되기 전에 지속적으로 이와 같은 요청이 아주 빠르게 이루어진다면 SYN packet은 backlog queue에 쌓이게 되어 결국 메모리 용량을 넘어서게 되면 해당 포트에 대한 연결을 받아들일 수 없는 상태인 서비스 거부상태가 된다.

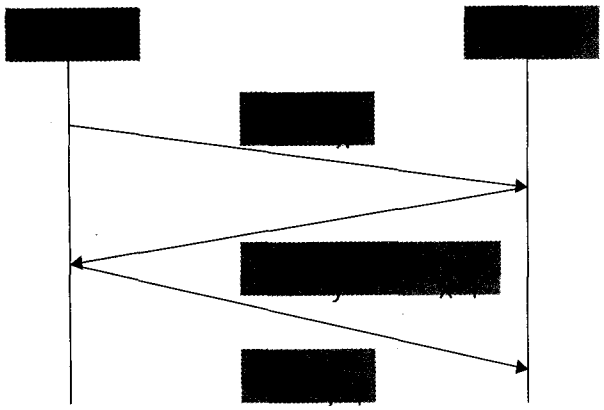


그림 2. 3 way-handshake
Fig. 2. 3 way-handshake

3.2 TCP SYN Flooding Attack의 해결 방안

TCP SYN flooding attack에 대하여 이미 알려져 있는 대안은 다음과 같다.

1. Backlog queue

실제 서비스 거부가 발생하는 원인으로 backlog queue에 더 이상 받아들일 수 있는 조건이 되지 않기 때문이다. 이를 해결하기 위해서 backlog queue 크기를 증가시켜주는 방법이다. 그러나 H/W 및 OS마다 서로 다른 메모리 용량과 backlog queue 크기가 할당되어 있어 정확한 크기 증가 선정이 어려워진다. 그리고 이러한 대안은 지속적인 공격과 비용측면에서 볼 때 효율적이지 못하므로 적절한 대안이라 할 수 없다.

2. Syncookies

Syncookies에는 크게 Berkeley, Linux, Reset cookie가 있으며 '3 way_handshake'에서 TCP header의 SYN's sequence number, 소스 및 목적 주소에 단 방향 해쉬 함수를 적용한 암호화 알고리즘을 이용한 방식으로 연결 설정이 정상적으로 이루어지지 않으면 더 이상 소스 경로를 따라 가지 않고 정상적 연결 요청에 대해서만 연결 설정을 하여 자원의 낭비를 줄이는 방법이다. 이 방법은 backlog queue 가 가득 쌓였을 경우에도 정상적인 접속 요구를 계속 받아들이므로 SYN flooding attack 에 가장 효율적인 방법 중 하나이다.

3. Packet monitoring

라우터 및 게이트웨이를 통과한 후 시스템 접근에 앞서서 모니터링을 하는 방법으로써 들어오는 패킷을 캡쳐하여 분석한 후 'half open state'를 요청하는 포트 및 IP address를 탐지하여 RST 등으로 연결 해제하는 방법이다[4][5]. 본 논문에서 제안하는 모니터링을 통한 알고리즘의 적용 또한 이 범주에 속한다.

3.3 SYN Flooding Attack에 대한 Positive Selection 알고리즘.

앞에서 제시한 packet monitoring을 이용하여 캡쳐 및 분석된 패킷에서 MHC 단백질로 삼는 데이터는 정상적인 패킷의 SYN과 RST, 그리고 sequence number이다[1]. 이때 새로이 유입되는 패킷에서 RST bits 값과 SYN bits, 그리고 sequence number bits 값을 MHC set과 매칭 후 일치하는 데이터는 MHC set을 업 데이트 하는데 이용하고, 일치하지 않는 데이터는 알고리즘에 제시된 방법으로 처리한다.

이에 대한 알고리즘은 다음과 같으며 그림 3은 알고리즘의 개념도이다.

① 패킷을 Capture한다.

② 패킷을 분석한다.

③ 정상적인 패킷에서 추출된 데이터를 이용하여 self string set을 설정한다. 추출된 데이터란 파싱된 패킷의 데이터들로써 local port, IP Address, Sequence number, window size, RST, FIN, SYN, Half Port Scan 등을 의미한다.

④ Self string set을 바탕으로 MHC set을 초기화 한다. MHC set은 self string set을 이용하여 구성한다. MHC set은 MHC 단백질에 대응되는 데이터는 패킷의 구성 성분인 SYN bits, RST bits 그리고 Sequence number를 포함하는 string이다. 여기서 MHC set은 BIS의 세포독성 T세포의 역할을 하게 된다[2][3].

⑤ 새로이 유입되는 패킷을 분석한 후 MHC set과 matching 후 일치하는 경우에는 MHC set을 업데이트 하게 되며 그렇지 않을 경우에는 전송제어 또는 전송오류제어에서 사용하는 방식인 윈도우 크기를 조절하여 현재의 세션을 중지 시켜서 SYN Flooding Attack 에 대처한다. 이때 매칭이라 함은 MHC 단백질로 설정한 bits 들이 MHC set과 일치하는 지 여부를 가리는 것이다. 매칭에 사용되는 선택 방법은 positive selection이다.

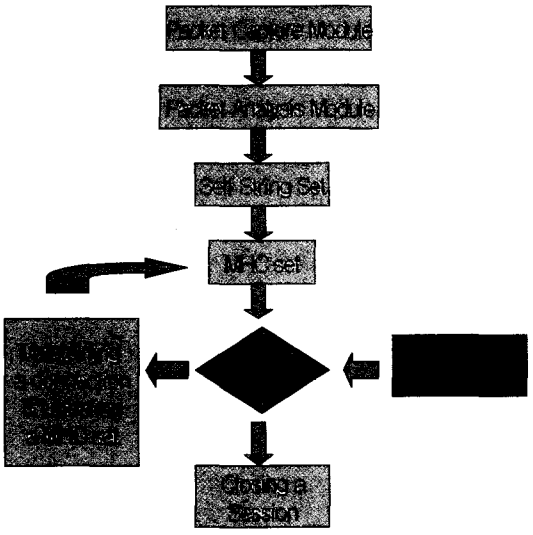
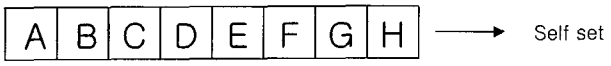


그림 3. Positive Selection 알고리즘의 개념도
Fig 3. Conceptional diagram of Positive Selection Algorithm

3.4 Simulation

본 논문에서 self set의 크기는 시뮬레이션을 위해서 기본적으로 64 바이트이다. 그 내용은 패킷 분석모듈에서 parsing 된 것들로 구성되어 있다. 그림 4는 그 self set의 구성을 보여준다. A, C, D 비트들은 BIS의 MHC 단백질의 역할을 한다. 그들은 새로운 패킷에 위치하게 될 것이다. 왜냐하면, 패킷의 유입은 MHC set에 의해 결정되기 때문이다. 각 구성 요소들의 내용은 다음과 같다.



A - Sequence number bits
B - Ack number bit
C - RST bit
D - SYN bit
E - FIN bit
F - Window bit
G - Check sum bits
H - index bits

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

표 1은 새로운 데이터와 MHC set과의 매칭된 횟수를 보여준다. 각 매칭 루프마다 1,000번의 매칭이 이루어졌다. 매칭 루프의 횟수는 100번이었고 총 매칭 시도 횟수는 100,000번이다. 새로운 데이터에 대한 MHC set의 매칭은 기술한 MHC 단백질을 새로운 데이터가 포함하고 있을 때만 이루어진다. 그 값의 범위는 4에서 크게는 19까지이다. 시뮬레이션의 결과에서처럼, 그 둘 간의 매칭률은 BIS의 positive selection을 사용하였을 경우 매우 낮게 나타났다. 이것이 의미하는 바는 새로운 데이터가 MHC 단백질에 해당하는 비트들을 소유하지 못하였을 경우에는 시스템으로의 유입이 매우 힘들어진다는 것을 의미한다[3][6][8].

표 1. 매칭 회수
Table. 1 Matched Numbers

	최소 매칭 횟수	최대 매칭 횟수	총 합	평 균
매칭횟수/ loop	4 / 1 loop	19/ 1 loop	1,005/ 100 loop	1,005/ 100,00 =10.5

1 loop=1,000 번

4. Negative Selection 알고리즘

면역계에서, self와 nonself 객체들은 펩티드이며 아미노산으로 된 짧은 스트링들이다. 컴퓨터 시스템에서 대응되는 요소들을 위치시켜야만 하는 레벨이 어떤 객체인지는 정확하지 않다. 예를 들어, self 객체들은 시스템 상에서 자신들의 audit trail의 일부 랜덤한 부분을 검색하는 각각의 detector를 지닌 로그온 한 사용자들이 될 수 있다[5][6]. 그러나, 더욱 낮은 레벨의 객체가 강조되어 왔으며, detector들과 방어되어야 할 데이터들 모두는 대개 binary로 구성된 알파벳 심볼들에서 고정된 길이의 스트링들로 구성되어 있다. 그러나. 그 방식은 이런 표현에 의존하지 않으며, 어느 객체들의 집합체에 적용될 수 있다. 면역계에서, 항원과 T세포 수용체들을 결합시키는 것은 항원의 상호 보완적인 형태와 수용체 분자들 간의 상호 작용에 의존한다. 그들 간의 매칭은 정확할 필요는 없기에 각각의 수용체는 작은 범위의 유사한 항원들과 결합할 수 있으며 반대의 상황도 마찬가지이다.

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. 이

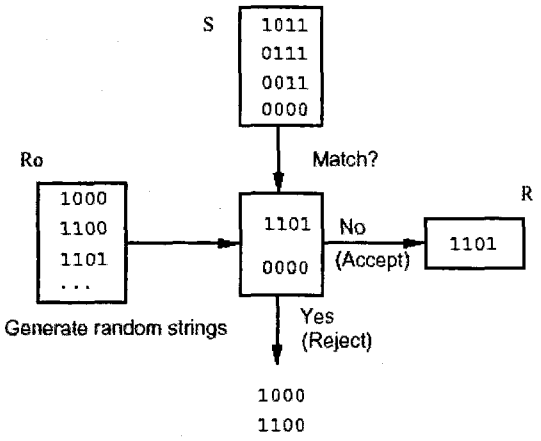


그림 5. 셀프스트링 S에서 디텍터 R 만들기
Fig. 5 Constructing a set of detectors R for a set of self strings S

때 사용되는 선택 방법이 negative selection이다. 이 과정은 요구되는 방어 수준에 이를 때까지 계속된다.

그림 5에 그 알고리즘이 나와 있다. 랜덤하게 생성된 스트링, R0 은 이미 설정해 두었던 self 스트링, S와 매칭을 하게 된다. 이때 self 스트링과 패턴이 같다고 판단되었을 경우에는 reject시키고 그렇지 않고 새로운 패턴일 경우에만 accept를 시킨 후, 기존의 detector, R을 갱신하는 데 사용된다. 즉, 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.

최근에 발생하고 있는 침입시도 및 바이러스의 경우 기존의 방식과 다른 새로운 시도들이 많이 발생하고 있다. 상업적으로 유포되는 침입 탐지 및 바이러스 탐지 프로그램들은 특정 징후에 대한 탐지 방식이라 변이된 침입 시도 및 바이러스에 대한 대처 방안은 미미한 실정이다. 하지만, negative selection을 이용하는 anomaly detector의 활용은 앞으로 이 문제점들에 대해 충분한 방편이 될 것이다[3][7][8].

5. Positive selection과 Negative selection의 혼용 알고리즘

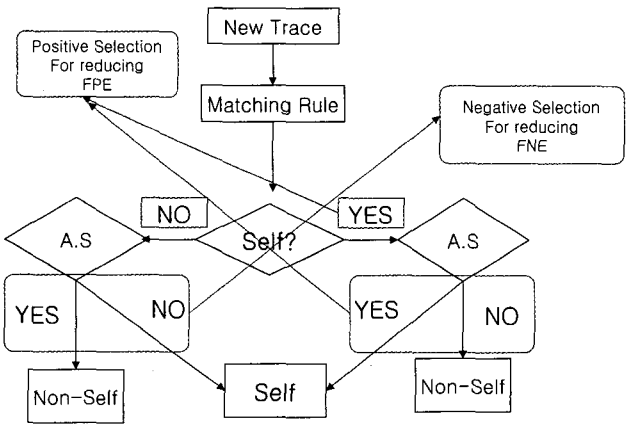
침입탐지 시스템은 분석 대상에서 추출한 정보를 이용해서 침입 여부를 판단하는데, 탐지 방식에 따라 오용탐지(misuse detection) 방식과 비정상행위 탐지 (anomaly detection)방식으로 나눌 수 있다. 오용탐지 방식은 알려져 있는 공격 행위로부터 특정 signature를 추출해내고, 분석 대상에 그런 signature가 존재하는지를 확인하여, 존재할 경우 침입임을 판단하는 방식이다. 그렇기 때문에 알려져 있는 공격에 대한signature 목록을 유지해야 하고, 이 목록을 얼마나 최신의 버전으로 유지하느냐에 따라 새로 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 number를 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.

본 논문에서는 앞에서 언급한 두 가지 방식을 혼용하기 위해 그림 6의 알고리즘을 제안한다. 매칭 규칙(Matching Rule)을 거친 self 데이터는 두 번의 선택을 거치게 되는 데, 첫 번째는 positive selection이며 두 번째는 negative selection이다. positive selection을 거친 데이터는 기준에 따라 잠정적으로 self 후보군과 nonself 후보군으로 나뉘게 된다. 두 번째는 negative selection을 거치게 되는 데, 이 때 사용되는 매칭 기준이 Anomalous Standard(A.S)이다. A.S는 1차 단계를 거친 데이터에 대해서 False Positive Error(FPE)와 False Negative Error(FNE)를 줄이기 위한 단계이며, 아울러 생체 면역계의 면역세포 형성원리인 negative selection을 모델링한 것이다.

일반적으로 비정상행위 탐지 방식은 오용탐지 방식에 비해 상대적으로 False Negative율이(nonself를 self로 인식하는 경우) 낮은 반면 False Positive율이(self를 nonself로 인식하는 경우) 너무 높아서 실제 환경에서 사용하기가 힘들었기 때문에, 주로 연구 범주에 많이 머물러 있었고, 상용 침입탐지시스템에 적용되지 못했었다. 최근에는 이런 비정상행위 탐지 방식에 대한 연구가 많이 이루어져서 비정상행위 탐지 방식에 기반 한 침입탐지 시스템이 많이 개발되는 편이지만, 기존의 상용 침입탐지 시스템은 오용탐지 방식의 한계를 극복하기 위해 부분적으로 제한적인 비정상행위 탐지 방식을 채용하고 있다. 이에 반해 본 논문에서 제안한 혼용 알고리즘은 이들의 취약점을 보완하고자 그 둘 간의 채택 비율을 유사하게 하였다. 이는 기존의 침입 시도 및 바이러스에 대한 탐지를 가능케 함은 물론이고, 변이된 침입 시도 및 바이러스에 대한 탐지를 목표로 하고 있다.



A.S: Anomalous Standard
FPE: False Positive Error
FNE: False Negative Error

그림 6 혼용 NIDS 알고리즘의 개략도
Fig. 6 *Conceptional diagram of Hybrid NIDS Algorithm*

6. 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 생성과정을 즉, positive selection과 negative selection을 이용한 알고리즘은 정상적인 접근에 대한 인식과정과 비정상적인 침입에 대한 이중적인 인식과정을 거치기 때문에 침입탐지의 신뢰도를 향상시킨다.

참 고 문 헌

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

[2] 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.

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

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

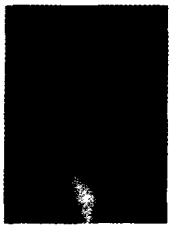
[5] C. Warrender, S. Forrest, B. pearmutter, "Detecting intrusions using system calls: Alternative data models," IEEE Symposium on security and Privac, 1999.

[6] S. Hofmeyr, S. Forrest, and A. Somayaji, "Intrusion Detection Using Sequence of System Calls." Journal of Computer Security, vol. 6, pp. 151-180, 1998.

[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
1997년~현재 한국퍼지 및 지능시스템학회 편집이사 및 논문지 편집위원장

2000년~현재 제어자동화시스템공학회 이사 및 직선평위원
2000년~현재 대한전기학회 제어및시스템부문회 편집위원 및 학술이사
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(Jea-Won Yang)

2002년 : 중앙대학교 전자전기공학과 공학사
2002년 : 동 대학원 전자전기공학과 공학석사

관심분야 : Network Security, 인터넷 정보보호, Computer Network, 진화연산
Phone : +82-2-820-5319
Fax : +82-2-817-0553
E-mail : emfvnf@jupiter.cie.cau.ac.kr

이동욱(Dong-Wook Lee)

1996년 : 중앙대학교 제어계측공학과 공학사
1998년 : 동 대학원 제어계측학과 공학석사
2000년 : 동 대학원 제어계측학과 공학박사

관심분야 : 인공생명, 진화연산, 인공면역계, 인공두뇌 등
Phone : +82-2-820-5319
Fax : +82-2-817-0553
E-mail : dwlee@ms.cau.ac.kr

서동일(Dong-Il Seo)

1989년 : 경북대학교 전자공학과 공학사
1994년 : 포항공과대학교 정보통신학과 공학석사
2002년 : 충북대학교 전자계산학과 (박사과정 수료)
1989.1~1992.2 : 삼성전자 종합연구소
1994.3~현재 한국전자통신연구원 사이버테러기술분석팀장

관심분야 : Network Security, 인터넷정보보호, Computer Network
Phone : +82-42-860-3814
Fax : +82-42-860-5611
E-mail : bluesea@etri.re.kr

최양서(Yang-seo Choi)

1996년 : 강원대학교 전자계산학과 이학사
2000년 : 서강대학교 컴퓨터공학과 공학석사
2000. 6~현재 한국전자통신연구원 사이버테러기술분석팀 연구원

관심분야 : Network Security, 인터넷 정보보호, Computer Network
Phone : +82-42-860-3982
Fax : +82-42-860-5611
E-mail : yschoi92@etri.re.kr