퍼지 및 지능시스템학회 논문지 2004, Vol. 14, No. 1, pp. 75-81

학습 알고리즘 기반의 적응형 침입 탐지 알고리즘

Adaptive Intrusion Detection Algorithm based on Learning Algorithm

심귀보* · 양재원* · 이동욱* · 서동일** · 최양서**

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

* 중앙대학교 전자전기공학부

** 한국전자통신연구원 네트워크보안구조 연구팀

요 약

징후 기반의 침입 탐지 시스템은 일정한 침입 탐지 규칙을 구성하여 라이브러리에 저장한 후 새로운 입력에 대해 규칙과 패턴 매칭을 하여 침입 여부를 판정한다. 그러나 징후(규칙)를 기반으로 하는 침입 탐지 시스템은 통상적으로 크게 2가지의 제약을 갖는다. 첫 번째는 침입에 대한 규칙을 구성하지 못할 경우 그에 따른 FN 오류(false negative error)가 발생할 수 있으며, 두 번째는 규칙의 다양성을 확보하기 위해서 많은 규칙을 구성하게 되었을 경우 그에 소요되는 자원의 규모가 커진다는 점이다. 이에 본 논문에서는 생체 면역 세포의 생성 과정인 부정 선택을 공학적으로 모델링하여 변형 인식부를 구성하고 이를 후보 개체군으로 하여 유전자 알고리즘을 이용해 진화시킴으로서 변이적인 침입에 대해 탐지 가능한 변형 인식부의 학습 알고리즘을 제안한다. 제안한 알고리즘은 컴퓨터 시뮬레이션을 통하여 그 유효성을 입증한다.

Key Words : 침입 탐지, 부정 선택, 변형 인식부, 유전자 알고리즘, 학습

Abstract

Signature based intrusion detection system (IDS), having stored rules for detecting intrusions at the library, judges whether new inputs are intrusion or not by matching them with the new inputs. However their policy has two restrictions generally. First, when they couldn't make rules against new intrusions, false negative (FN) errors may are taken place. Second, when they made a lot of rules for maintaining diversification, the amount of resources grows larger proportional to their amount. In this paper, we propose the learning algorithm which can evolve the competent of anomaly detectors having the ability to detect anomalous attacks by genetic algorithm. The anomaly detectors are the population be composed of by following the negative selection procedure of the biological immune system. To show the effectiveness of proposed system, we apply the learning algorithm to the artificial network environment, which is a computer security system.

Key Words : intrusion detection, negative selection, anomaly detector, genetic algorithm, learning

1. 서 론

인간의 몸에는 외부로부터 병원균이 유입되거나 자기 조직에 적합하지 않는 세포가 유입되었을 경우를 대비하는 대응 시스템이 있다. 이것을 면역 시스템[1, 2]이라고 한다. 면역 시스템은 크게 두 가지의 시스템으로 구성 된다. 그 첫 번째는 선천성 면역(innate immunity)이고, 두 번째는 후천성 면역(acquired immunity)이다. 두 가지 시스템 모두가 백혈구의 활동에 의존한다는 공통점이 있지만 전자의 경우는 주로 과립성 백혈구와 대식세포의 도움으로 그 기능을 수행하며, 후자는 림프구라고 불리는 B 세포와 T 세포의 중재로 그 기능을 수행한다. 이 자연적인 방어 시스템의 기능은 정밀하면서도 외부의 공격으로부터 자신을 방어하는데 철저하다. 특히 B 세포와 T 세포가 행하는 적응 면역시스템을 공학적으로 모델링하는 연구가 최근 활발히 진행되고 있다[3-8].

그 중 T 세포의 생성 과정의 일부인 부정 선택(negative selection) 메커니즘을 모델링 하는 연구가 대표적이다. Forrest[5] 등은 그 메커니즘을 네트워크 기반의 컴퓨터 바이러스 탐지에 적용하였고, D'haeseleer[6] 는 자기-비자기(self-nonself) 식별 문제를 해결하기 위한 알고리즘을 제시하였다. 한편 Kim과 Bently[7, 8]는 네트워크 트래픽 변형 인식부(network traffic anomaly detector)를 생성하기 위하여 그 메커니즘을 사용하였고, 적절한 수의 인식부 생성과 외부 공격의 표본 크기를 제시하기 위해서 사용하였다. 또한 네트워크 환경에서 유입되는 패킷(packet)을 대상으로 침입을 탐지하기 위한 알고리즘을 제시하기 위해서 동일한 메커니즘을 사용하였다. 본 논문에서도 부정 선택 메커니즘을 바탕으로 자기와 비자기의 구분을 위한 초기 변형 인식부를 생성한다. 하지만 여기에 유전자 알고리즘을 이용한 학습 알고리즘을 추가함으로서 적절한 인식부의 수를 유지하고 적응적

접수일자 : 2004년 1월 5일
완료일자 : 2004년 2월 6일
감사의 글 : 본 연구는 한국전자통신연구원의 인공면역계 기반 적응형 침입탐지 알고리즘 연구의 위탁과제로 수행되었습니다. 연구비 지원에 감사드립니다.

인 침입 탐지가 가능하도록 하였다.

변형 인식부를 이용하여 침입 여부를 판단할 수 있는 기능은 기존의 연구별로 다양하지만 그 중에서 대표적인 알고리즘으로 Forrest가 제시한 r-인접 비트 매칭 함수(r-contiguous bits matching function)가 있다. 이는 제시된 두 개의 스트링이 최소한 r 개 이상은 일치되어야만 한다는 규칙으로서 현재 구성되어진 자기 시스템의 특성을 지니고 있는지 여부에 대한 문턱값이다. Kim과 Bently[7] 역시 r-인접 비트 매칭 함수를 이용하여 유사성의 정도를 측정하여 침입 여부를 판단하고 있다. 그러나 그들은 r-인접 비트 매칭 함수의 적용이 범용적이지 못함을 지적하기도 하였다. 한편 본 저자들은 면역 세포의 생성과정인 부정 선택과 긍정 선택을 이용한 변경검사 알고리즘 및 침입탐지 시스템을 제안하였다[9-11].

면역 세포의 유전자 세크먼트의 협조적 매칭을 이용한 진화적 접근 방식이 이미 Dasgupta[12]에 의해서 제안되었다. 그 방식은 적합도 함수를 계산하기 위하여 개체군내에 있는 상위 x%의 개체들이 항원(nonself)으로 선택되어지며, 이 항원과의 친화도를 이용한다. 또한 Kim와 Bently[8]들도 네트워크 침입 탐지를 위해 진화 모델을 도입하였다. 그들은 이미 자신들의 데이터 분류법으로 r-인접 비트 매칭 함수를 이용하여 네트워크 적체 현상을 탐지하는 알고리즘을 제안하였으나 그 유효성에 한계를 극복하고자 데이터 분류방식으로 진화모델을 적용하였었다.

본 논문에서는 부정 선택 방법에 의해 생성된 변형 인식부를 다양성을 유지하면서 변화하는 환경에 대응할 수 있도록 유전자 알고리즘을 도입하였다. 시뮬레이션을 통하여 변화하는 침입에 대하여 탐지가 가능할 수 있는지 여부에 대해서 확인하였다.

2. 연구 배경

2.1 침입 탐지 시스템

침입 탐지 시스템(IDS: intrusion detection system)[13]은 기본적으로 데이터 수집(data collection), 데이터 분류(data classification), 데이터 보고(data reporting)의 3가지 요소를 가진다. 또한 시스템의 특징에 따라 여러 가지 형태로 나누어 볼 수 있다. 우선 관리방식에 따라 침입 탐지 기능이 여러 컴퓨터에 분산된 분산형 시스템과 하나의 시스템에서 관리하는 중앙 집중식 시스템으로 나눌 수 있다. 기존에는 중앙 집중식 방식이 주로 사용되었고 최근의 연구에서 분산형 시스템에 대한 연구가 수행되고 있다. 두 번째로 네트워크의 이용 여부에 따라 호스트 기반(host based) 방식과 네트워크 기반(network based) 방식으로 나눌 수 있다. 전자는 한 대의 컴퓨터에서 발생하는 이벤트(event)에 대하여 모니터링을 수행하는데 반해 후자는 하나의 네트워크 전반에 걸쳐 발생하는 이벤트를 모니터링 한다. 아울러 후자는 서로 다른 많은 호스트로부터 유입된 audit trails와 대조된 정보를 모니터링 할 수 있거나 또는 네트워크 트래픽을 모니터링 할 수도 있다.

2.2 생체 면역 시스템

생명체의 방어체계인 면역 시스템[1, 2]은 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 바이러스 감염과 종양발생에 의해 변이한 자기세포를 배제하는 작용도 가지고 있다. 이러한 생명체의 면역계는 중앙 처리 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.

2.3 면역 세포의 형성 원리

생체 면역 시스템에서 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 세포와 구별되는 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(MHC: major histocompatibility complex)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 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 항원 수용체의 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 항원수용체의 정상적인 동작여부를 확인하면서 면역 세포를 생성하여 면역계를 구성한다. 수용체의 정상적인 동작여부를 가리는 방법으로 사용되는 것이 긍정 선택(positive selection)과 부정 선택(negative selection)이다.

부정 선택은 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. 이 때 긍정적인 선택을 하는 면역세포는 MHC 단백질을 항원으로 인식하는 세포들이므로 죽이거나 다시 항원 수용체를 형성하는 단계를 거치게 된다.

긍정 선택은 각 면역세포의 MHC 인식기능을 확인하는 선택 방법이다. 자기세포에서 분비되는 MHC 단백질을 정확

히 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.

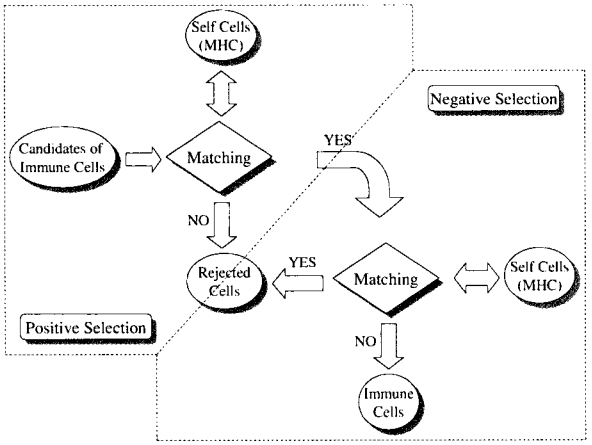


그림 1. 면역 세포의 형성과정
Fig. 1. The formation procedure of immune cells

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 보여준다.

3. 학습 알고리즘 기반 적응형 침입 탐지 알고리즘

3.1 Snort를 이용한 침입 탐지 시스템

본 논문에서는 제안한 알고리즘을 검증하기 위하여 Snort[14, 15]라는 침입탐지 프로그램을 사용하였다. Snort는 오용탐지 시스템으로서 규칙 기반이자 네트워크 기반의 시스템이다. 또한 공개용 침입탐지 시스템으로서 상용프로그램에 뒤떨어지지 않으며 자유롭게 이용이 가능하다. 이것은 1998년 Roesch가 APE라고 불리는 리눅스용의 sniffer로 만든 것을 패킷 sniffer, 패킷 logger와 네트워크 침입탐지를 수행하도록 확장한 것이다. 패킷 sniffer로써의 snort는 다음과 같은 기능을 갖는다[12].

Snort는 징후(signature) 기반 침입탐지 시스템으로서 임의의 네트워크에서 잘못된 패킷들을 체크하기위해서 규칙 집합(rule set)을 이용한다. 규칙이란 'alert'를 조절하게 될 요구사항들의 집합을 의미한다. 예를 들어, peer-to-peer file sharing service를 체크하기위한 하나의 snort rule은 port 80에서 운영되고 있는 서비스에 연결되지 않고 있는 GET string을 체크하게 된다. 만약 한 패킷이 이 규칙과 매칭이 되면 그 패킷은 'alert'를 만들어낸다. 일단 'alert'이 만들어지게 되면, 그 alert은 log file, database 그리고 SNMP trap과 같은 다중의 장소로 전달이 되어질 수 있다.

그 규칙의 구조는 (헤더 + 옵션)으로 되어 있다. 예를 들면 다음과 같다.

alert tcp $EXTERNAL_NET 27374 -> $HOME_NET any *(msg:" BACKDOOR subseven 22"; flow:to_server,established; content: "|0d0a5b52504c5d3030320d0a|";*

위의 예에서 볼드체 부분이 규칙의 헤더(rule header)로써 tcp 프로토콜의 외부 27374포트에서 내부의 임의의 포트로 유입되는 패킷들을 탐지한다는 의미이다. 이탤릭체 부분은 규칙의 옵션(rule option)부분으로 예에서는, 내부의 임의의 포트로 들어오는 패킷 중 내용이 /0d0a5b52504c5d3030320d0a/이면, 즉 패킷이 규칙과 일치할 경우에는 침입탐지로 간주하고 BACKDOOR sub_server 22라는 메시지를 보이며 로그를 남긴다.

이와 같이 각각의 침입에 대비한 규칙 집합을 signature형식으로 라이브러리로 저장한 후, snort프로그램 구동시, snort.conf 파일에서 탐지해야할 signature 별로 해당 규칙 집합을 옵션으로 설정해주게 되면, 유입되는 패킷을 분석하여 매칭을 실시한다.

3.2 변형 인식부의 코딩방법

인식부를 자동 생성하고 적응적으로 변화시키기 위하여 비트 스트링으로 코드화 하였다. 비트 스트링으로 표현함으로서 부정 선택방법을 이용해 변형 인식부를 생성 할 수 있으며 유전자 알고리즘의 염색체로도 그대로 사용할 수 있다.

침입 탐지 시스템에서 자기와 비자기를 구별하는 인식부는 snort의 분류규칙(classification rule)이다. 본 논문에서는 부정 선택을 통해 생성한 규칙을 특별히 변형 인식부라고 명명 한다. Snort는 규칙을 기반으로 하는 체인 매칭 방식의 침입 탐지 시스템이다. 정의된 규칙의 모든 패턴과 일치하는 패킷을 침입으로 판정한다. 정의된 규칙과 하나의 패턴만 달라도 침입으로 판정하지 않는다. 따라서 대부분의 침입 패턴에 적용될 수 있는 옵션을 선정하여야 한다. 일반적으로 사용되는 방법으로 규칙 헤더와 규칙 옵션을 사용하는데 이때 규칙 헤더에서 중요한 정보는 내부로 데이터가 유입되는 포트의 넘버이다. 그리고 규칙 옵션에서 중요한 정보는 content에 해당되는 데이터가 된다. 본 연구에서 이 두 가지 데이터를 이용하여 규칙을 인코딩 하였다. 그림 2에서 제시된 content 1~3 은 각각 그 포트에서 유입되는 패킷이 가질 수 있는 데이터 값의 범위를 나타낸다.

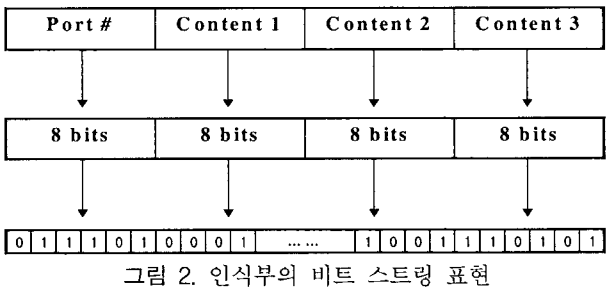


그림 2. 인식부의 비트 스트링 표현
Fig. 2 Bit string representation of a detector

그림 2에서 port #는 해당 프로토콜 별로 사용되고 있는 포트 번호(port number)를 의미하며 그 길이는 8 비트가 된다. 다음의 content 1~3은 캡쳐한 패킷에서 탐지를 수행할 데이터를 의미하는 것으로 규칙의 구조에서 언급한 것처럼 규칙의 옵션에 해당되는 데이터를 의미하며 각각 8 비트가

할당된다.

3.3 부정 선택 방법에 의한 변형 인식부 생성

흉선에서 T 세포를 생성하는 것과 같이 초기 인식부 스트링을 랜덤하게 생성한다. 이때 자기 자신을 항원으로 인식하는 세포들은 제거될 필요가 있는데, 보호되어야 할 자기 스트링들과 매칭을 하여 매칭되는 것들은 제거한다. 이때 자기 스트링들과 매칭 되는데 실패한 것들로만 인식부 집합, R을 구성한다. 이때 사용되는 선택 방법이 부정 선택이다. 이 과정은 충분한 인식부가 얻어질 때까지 계속한다.

그림 3은 부정 선택에 의해 인식부 집합 **R**을 구성하는 방법을 보여준다[5]. 우선 랜덤하게 생성된 스트링, $\mathbf{R_0}$를 이미 설정해 두었던 자기 스트링, S와 매칭을 시킨다. 이때 자기 스트링과 패턴이 같다고 판단되었을 경우에는 거절(reject)시키고 그렇지 않고 새로운 패턴일 경우에만 승낙(accept)시켜 인식부 집합 **R**을 구성한다.

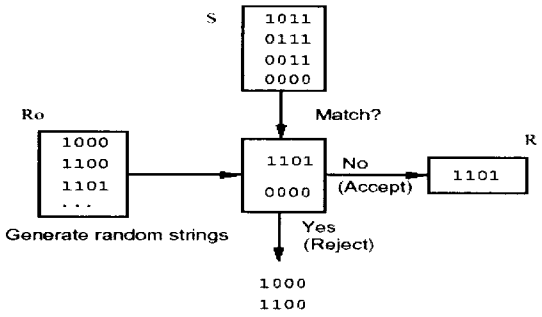


그림 3. 부정 선택에 의한 인식부의 구성[5]
Fig. 3 Constructing a set of detectors by negative selection [5]

본 방식의 가장 큰 특징은 알려지지 않은 침입에 대해 충분한 인식부를 구성함으로서 대처 할 수 있다는 점이다. 기존의 인식부(침입 탐지 규칙)의 구성방법은 이미 침입을 당한 이후 알려진 침입패턴에 대하여 대응하는 규칙을 생성하는 방법이다. 이것은 기 알려진 침입에 대해서는 효과가 있으나 변경된 침입이나 전혀 새로운 침입에 대해서는 효과가 없다. 따라서 본 논문에서 제안된 알고리즘은 기존의 방식에 추가하여 새로운 침입을 탐지하는 방법으로 매우 유용하게 사용될 수 있다.

하지만 본 방법은 정상적으로 접근하는 데이터 패턴 즉 자기 스트링을 충분히 확보하여야 하며 새로운 칩입에 대처하기 위한 많은 수의 인식부를 준비해야 하는 단점을 가지고 있다. 다음 절에서는 많은 수의 인식부를 준비해야 하는 단점을 극복하고 환경에 적응할 수 있는 인식부 집합을 구성하는 방법을 제안한다.

3.4 인식부의 적응적 진화 모델

침입탐지는 주로 침입을 탐지하기 위한 인식부를 구성하는 방법으로 이루어진다. 기존의 방식에서는 인식부의 수가 한번 결정되면 항상 일정한 수로 제한되기 때문에 인식부가 인식하지 못하는 보안의 허점이 발생할 가능성이 있다. 이에 대한 해결책으로 인식부의 수를 늘이는 것은 계산상의 비용을 증가시켜 적절한 방법이 아니다. 본 연구에서는 이와 같은 문제점을 해결하기 위하여 인식부의 수를 적절하게 유지하면서 새로운 변화에 적응할 수 있도록 인식부를 진화시키는 방식을 사용한다.

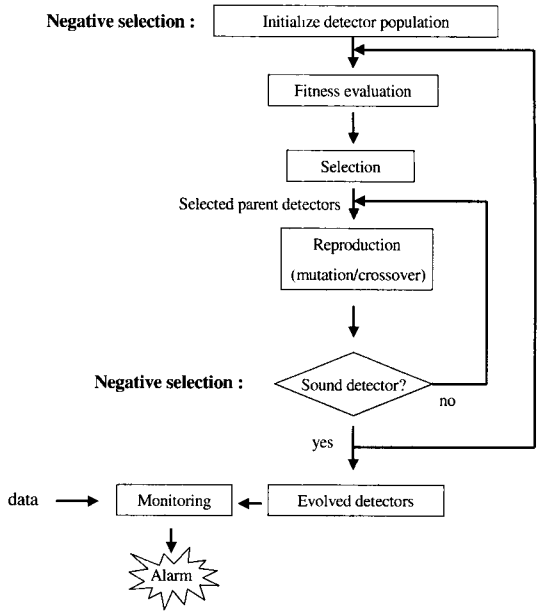


그림 4. 인식부의 적응적 진화모델
Fig. 4. The adaptive evolutionary model of receptors

그림 4는 인식부의 진화를 통한 침입탐지 시스템의 개요도 이다. 먼저 인식부의 초기 개체군을 만들고 데이터를 통해 적합도를 결정한다. 초기개체군은 부정선택 방법에 의하여 자신(정상)을 침입으로 간주하지 않는 인식부들로 구성한다. 적합도는 적합도 할당(fitness sharing)[16]에 기반한 (1)식에 의해 평가한다. 인식부의 적합도가 결정되면 적합도에 따라 인식부를 선택하고 재생산 한다. 재생산된 인식부에 의해 입력되는 데이터를 모니터링한다. 이때 인식부의 선택은 적합도 비례로 2개를 선택하여 재생산하고 최하위 적합도의 두개의 인식부를 제거한다.

$$f_i = \frac{g_i - k}{\sum_{j=1}^{n} sh(d_{ij})} \tag{1}$$

단, g_i은 과거 일정 기간동안의 항원(침입)에 대한 인식률, k는 시간에 따라 적합도를 감소시키는 나이계수(age coefficient), n은 개체수, $sh(d_{ij})$는 현재 인식부간의 공유상태를 나타내는 식으로 다른 인식부와 인식부의 다양성을 나타내는 지수를 나타내며 (2)식과 같이 정의된다.

$$sh(d_{ij}) = \begin{cases} 1 - \dfrac{d_{ij}}{\sigma_s}, & \text{for } 0 \le d_{ij} < \sigma_s \\ 0, & \text{for } d_{ij} \ge \sigma_s \end{cases} \tag{2}$$

(2)식은 개체 i와 j의 거리(해밍 디스턴스)를 나타내는 d_{ij}를 이용해서 각 개체가 공유거리 내에 들어와 있는 정도를 합산한 값이다. 이때 σ_s는 공유거리의 범위를 정하는 파라미터 이다. (2)식에 의해 (1)식의 적합도는 주어진 인식부가 다른 인식부와 거리가 멀수록 높아지고 작을수록 낮아진다. 따라서 인식부의 다양성을 증가시키는 역할을 한다.

재생산(reproduction)과정에서는 선택된 두 부모 인식부를

이용해 두개의 자식 인식부를 생성한다. 이때 생성된 자식 인식부는 아직 인식부로서 검증이 안 된 것이므로 부정선택 방법에 의해 정상적인 데이터에 적용시켜 잘못된 인식부가 얻어질 경우 재생산의 과정을 다시 거친다. 이때 정상적인 두개의 인식부가 얻어질 때까지 재생산 과정(돌연변이 및 교차 연산수행)을 반복한다.

4. 실험 결과

본 실험에서는 부정 선택 방법과 인식부의 진화모델을 이용해 snort의 규칙을 생성하고 생성된 규칙을 이용하여 침입 탐지를 수행하였다.

실험은 그림 4의 순서에 따르며 구체적인 내용은 다음과 같다.

첫 번째로 정상적인 접속 연결을 한 데이터를 수집해 자기 공간(self space)을 구성한다.

두 번째로 3.3절에 설명된 부정 선택 방법에 의하여 인식부의 초기개체군을 생성한다. 즉, 초기개체를 랜덤 생성시켜 자기공간의 데이터와 비교해 정상적인 연결을 침입으로 인식하지 않는 개체들만을 선택한다. 이때 선택된 개체들은 정상적인 연결을 침입으로 인식하지 않는 규칙들의 후보가 된다. 본 실험에서 개체군의 크기는 100과 200의 두 가지 경우에 대하여 실험하였다.

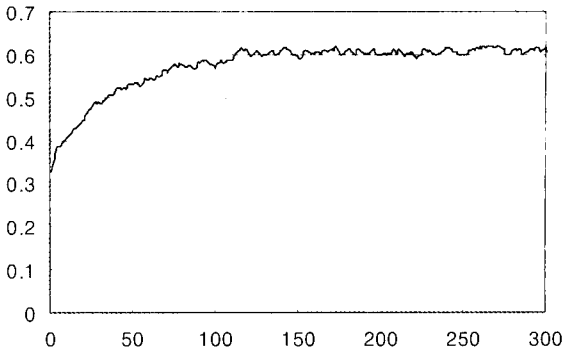
세 번째로 생성된 각 개체들은 침입연결을 포함한 데이터를 적용시켜 적합도를 평가한다. 적합도는 초기 개체군을 통해 얻어진 규칙집합을 이용해 침입탐지를 수행하고 이때 얻어진 로그파일을 분석하여 계산한다.

네 번째로 계산된 적합도를 기반으로 재생산(교차 및 돌연변이 연산)을 수행한다. 이때 교차율은 0.5, 돌연변이율은 0.04를 사용하였다.

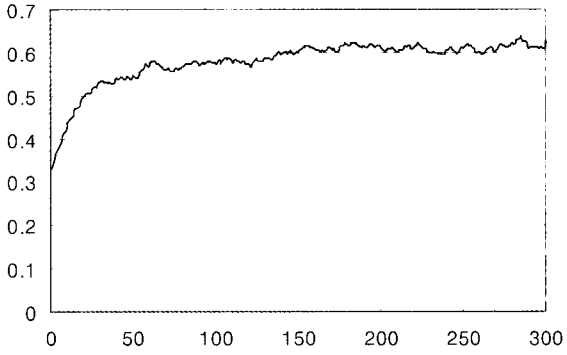
다섯 번째로 재생산된 개체의 정상적인 연결(자기 공간)의 인식여부를 부정 선택 방법에 의해 검사하고 만약 정상적인 연결을 침입으로 잘못 인식할 경우 제거하고 다시 네 번째 단계의 재생산을 거친다. 이후 세 번째에서 다섯 번째 단계를 들어오는 데이터에 대하여 계속적으로 수행한다.

본 알고리즘은 기존의 GA에서와 같이 일괄적으로 선택 및 재생산을 거치지 않고 시간에 따라 개체군의 개체 중 일부(1개 또는 2개)를 선택하여 재생산을 수행한다. 따라서 진화된 세대를 판단할 수 있는 세대 차이(generation gap)는 (1/개체군의 수) 가 된다. 즉 개체군의 크기가 100일 경우 100개의 개체가 재생산되면 1세대가 지난 것으로 간주 할 수 있다.

그림 5는 제안한 알고리즘의 유효성을 판단하기 위하여 시스템에 침입 패턴을 계속적으로 변화하면서 시도했을 때 본 알고리즘에 의한 침입 탐지율을 나타낸 그래프이다. 그림 5의 (a)와 (b)는 각각 인식부 개체군의 크기를 100개와 200개로 하였을 때의 실험결과를 나타낸다. 총 300세대가 지나는 동안의 변화를 관찰하였다. 실험을 통하여 제안한 알고리즘이 평균적으로 60%정도의 침입 탐지율을 나타냄을 알 수 있었다. 하지만 개체군의 크기가 100과 200의 각각의 경우에 최종 인식률의 차이는 거의 없었다. 부정선택법에 의해 생성한 초기의 인식부(초기 세대)는 약 32%의 탐지율을 나타낸다. 여기에 적응적 진화알고리즘에 의해 진화하여 약 100세대부터는 60%정도의 탐지율을 유지함을 볼 수 있다.



(a) 개체군의 크기가 100일 경우
(a) In case that the number of population is 100



(b) 개체군의 크기가 200일 경우
In case that the number of population is 200

그림 5. 실험 결과(가로축: 세대, 세로축: 탐지율)
Fig. 5. Experimental result (horizontal axis: generation, vertical axis detection rate)

개체군의 크기가 200일 경우에도 개체군의 크기가 100일 경우에 비해 큰 성능향상을 보이지 않는데 이는 최적의 개체군의 크기가 존재함을 나타낸다. 또한 제한된 개체군을 이용해서 알려지지 않은 모든 침입을 100%탐지하는 것은 불가능하며 본 실험에서는 진화적 학습알고리즘을 적용하기 전(초기 세대의 탐지율)에 비해 약 2배의 성능향상을 가져왔다.

Snort를 비롯해 기존의 침입탐지 시스템은 이미 알려짐 침입에 대한 규칙을 가지고 있어서 그와 동일한 침입이 발생시에 침입을 탐지해 낸다. 하지만 변형된 침입이나 새로운 침입에 대해서는 탐지해 내지 못한다. 본 연구에서는 규칙(인식부)을 생성하고 진화시킴으로서 알려지지 않은 침입에 대하여 탐지해 내는 알고리즘을 제안하였다.

본 알고리즘의 목적은 알려지지 않은 공격에 대해서 자기 시스템의 정의만으로도 학습을 통해서 공격을 탐지하도록 하는 것이다. 알려진 공격에 대해서는 snort식의 징후 기반 규칙 집합을 작성하여 대처하고 알려지지 않은 공격에 대해서는 제시된 알고리즘을 이용하여 대처하게 되는 하이브리드(hybrid) 침입탐지 시스템이 가능할 수 있다. 결론적으로, 알려지지 않은 공격에 대해서 기존의 징후 기반 침입 탐지 방식으로는 그 해당되는 규칙을 작성할 수가 없으며, 이는 공격에 대해서 무방비 상태를 의미한다. 이에 반해 제안한 알

고리즘은 부정 선택에 의해서 생성된 인식부를 GA 연산을 통해서 학습을 함으로서 일정 세대수가 지나게 될 때 알려지지 않은 공격에 대해서 침입을 탐지할 수 있는 성능을 가지게 된다. 또한 다양한 공격에 대해서 침입 탐지를 하게 하기 위해서 적합도 함수에 적합도 할당(fitness sharing) 기법에서 유래된 해밍 디스턴스(hamming distance) 측정을 개체에 적용함으로써 일정 32비트 스트링으로 개체들이 특정하게 수렴하는 것을 방지함으로써 인식부들의 다양성을 유지시킬 수 있다. 다시 말해서, 자기 시스템의 정의를 바탕으로 부정 선택 된 인식부들은 다양성을 유지하면서 알려지지 않은 공격에 대해 학습을 통해서 탐지를 수행할 수 있는 것이다.

5. 결 론

본 논문에서는 네트워크 침입탐지 시스템에 적용하기 위한 생체 면역계의 부정 선택 모델과 진화적 기법을 이용한 적응형 침입탐지 시스템을 제안하였다.

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 연구에서는 생체 면역계의 면역 세포의 생성과정을 모델링 하고 진화적 기법을 도입함으로서 컴퓨터 환경에서 발생된 바이러스 및 침입시도에 대해서 적응적으로 대처하는 알고리즘을 제안하였다. 기존의 징후 기반 침입 탐지 프로그램인 snort의 규칙을 하나의 비트 스트링으로 표현함으로써 진화 기법을 적용할 수 있었다. 실험을 통하여 알고 있지 않은 침입에 대하여 적응적으로 60%의 침입 탐지율을 얻을 수 있었다.

본 연구에서 제안한 진화적 기법에 의해 적응하는 인식부 집합은 변화하는 환경 및 데이터에 대하여 유연하게 대처가능하며 호스트 연합 방식[17]에 적응적 인식부 집합을 이용하면 보다 강건한 적응형 침입탐지 시스템을 설계할 수 있을 것이다.

참고문헌

[1] R. A. Wallace, G. P. Sanders, and R. J. Ferl, *BIOLOGY: The Science of Life*, 3rd eds., Harper Collins Publishers Inc., 1991.

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

[3] D. Dasgupta ed, *Artificial Immune Systems and Their Applications*, Springer-Verlag, 1998.

[4] L. N. de Castro and J. Timmis, *Artificial Immune System: A New Computational Intelligence Approach*, Springer, 2002.

[5] S. Forrest, A.S. Perelson, L. Allen, and R. Cherukuri "Self-nonself discrimination in a computer," *Proc. of 1994 IEEE Symposium on Research in Security and Privacy*, pp. 202-212, 1994.

[6] P. D'haeseleer, "A distributed approach to anomaly detection," *ACM Transactions on Information System Security*, 1997.

[7] J. Kim, P.J. Bently, "Evaluating negative selection in artificial immune system for network intrusion detection," *Proc. of the Genetic and Evolutionary Computation Conference*, pp. 1330-1337, 2001.

[8] J. Kim, and P. J. Bentley, "Towards an artificial immune system for network intrusion detection: An investigation of clonal selection with a negative selection operator," *Proc. of Congress on Evolutionary Computation*, pp.1244-1252, 2001.

[9] 심귀보, 서동일, 김대수, 임기욱, "컴퓨터 면역시스템 개발을 위한 인공면역계의 모델링과 자기인식 알고리즘," *한국퍼지 및 지능시스템학회 논문지*, 12권, 1호, pp. 52-60, 2002. 2.

[10] 심귀보, 양재원, 이동욱, 서동일, 최양서, "생체 면역계를 이용한 네트워크 침입탐지 시스템," *한국퍼지 및 지능시스템학회 논문지*, 12권, 5호, pp.411-416, 2002. 10.

[11] 이동욱, 심귀보, "T세포 발생과정의 긍정 및 부정 선택에 기반한 변경 검사 알고리즘," *한국퍼지 및 지능시스템학회 논문지*, 13권, 1호, pp. 119-124, 2003. 2.

[12] D. Dasgupta, "Information processing in immune system," in D. Corne, M. Dorigo, and F. Glover (Eds.), *New ideas in optimization*, pp. 161-166. McGraw-Hill

[13] S. A. Hofmeyr, A. Somayaji, and S. Forrest. "Intrusion detection using sequences of system calls," *Journal of Computer Security*, vol. 6, pp 151-180, 1998.

[14] B. Caswell, J. Beale, J. C. Foster, and J. Posluns, *Snort 2.0 Intrusion Detection*, Syngress, pp.28-36. 2003.

[15] M. Roesch. *et al*, *Snort Users Manual Snort Release: 2.0.0*, 8th, 2003.

[16] D. E. Goldberg, *Genetic Algorithms in Search, Optimization, and Machine Learning*, pp. 189-192, Addison Wesley, 1989.

[17] J. B. Gu, D. W. Lee, K. B. Sim, and S. H. Park, "An immunity-based security layer against Internet antigens," *IEICE Trans. on Communications*, vol. E83-B, no. 11, pp. 2570-2575, 2000.

저 자 소 개

심귀보(Kwee-Bo Sim)

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

관심분야 : 인공생명, 지능로봇, 지능시스템, 인공두뇌, 다개체시스템, 자율분산로봇시스템, 기계학습 및 적응알고리즘, 소프트컴퓨팅(뉴로, 퍼지, 진화연산), 진화하드웨어, 인공면역스템, 침입탐지 등
Phone : +82-2-820-5319
Fax : +82-2-817-0553
E-mail : kbsim@cau.ac.kr

양재원(Jea-Won Yang)

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

관심분야 : Network Security, 인터넷 정보보호, Computer Network, 진화연산
E-mail : emfvnf@wm.cau.ac.kr

이동욱(Dong-Wook Lee)

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

2002년~현재 : 중앙대학교 정보통신연구원

관심분야 : 인공생명, 진화연산, 인공면역계, 인공두뇌 등
E-mail : dwlee@wm.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 네트워크보안구조연구팀장

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 네트워크보안구조연구팀 연구원

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