# 생체 면역 기반의 하이브리드 침입 탐지 시스템에 관하여

양은목* 이상용* 서창호** 김석우***
*공주대학교 정보통신공학부 **공주대학교 응용수학과,
***한세대학교 컴퓨터정보통신공학부

## 요 약

컴퓨터망의 확대 및 컴퓨터 이용의 급격한 증가에 따른 부작용으로 컴퓨터 보안 문제가 중요하게 대두되고 있다. 이에 따라 침입자로부터 침입을 줄이기 위한 침입탐지시스템에 관한 연구가 활발하다. 본 논문은 멀티레벨에서 감사자료를 수집하고, 필터링하여 오용행위 탐지기법에 대한 선천성면역, 비정상행위 탐지기법에 대한 후천성 면역을 사용한 하이브리드 침입탐지 시스템이다. 다중호스트 기반에서 감사자료를 하나의 시스템으로 모아서 탐지하므로 하나의 호스트에서 탐지한 침입보다 여러 호스트에서 탐지가 가능하며, 비정상행위 탐지 기법에서 탐지한 침입은 오용행위 탐지 기법에서 신속하게 탐지할 수 있는 면역력을 가진 침입탐지 시스템의 설계 및 구현한다.

# On the Hybrid Intrusion Detection System based Biometric Immuntiy

Eun-mok Yang* Sang-yong Lee* Chang-ho Seo** Seok-Woo Kim***

## ABSTRACT

Computer security is considered important because of the side effect generated from the expansion of computer network and rapid increase of the use of computer. Intrusion Dectection System(IDS) has been an active research area to reduce the risk from intruders. In this paper, the Hybrid Intrusion Detection System(HIDS) based biometric immuntiy collects and filters audit data by misuse detection is innate immune, and anomaly detection is acquirement immune in multi-hosts. Since, collect and detect audit data from one the system in mult-hosts, it is design and implement of the intrusion detection system which has the immuntiy the detection intrusion in one host possibly can detect in multi-hosts and in the method of misuses detection subsequently.

# 1. 서 론

인터넷과 네트워크 등과 같은 정보 기술의 발전과 활용으로 대부분의 시스템이 개방 환경에 노출되므로서 많은 장점도 있는 반면 크랙커(Cracker)의 침입으로 수많은 정보들이 개인의사와 무관하게 공개되고 있다. 이는 개인의 문제뿐만 아니라 사회의 문제로까지 야기되고 있다. 또한 크랙커의 침입이 있었는지, 어떤 행위를 했는지 일반 관리자들은 분석하기 힘들 정도로 더 치밀해지고 있다. 알려진 공격 방법에 대한 대응이 미비한 것과 알려지지 않은 방법들이 산재해 있는 것이 침입을 탐지하기 어렵게 하는 요소이다. 침입 탐지 시스템이 많이 개발되고 있지만, 침입이 아님에도 침입으로 통보하는 긍정적 결함(False Positive), 침입이 일어나고 있음에도 침입 패턴이 분석되지 않아 침입 경보를 알리지 않는 부정적 결함(False Negative)과 침입이 이루어져서 침입 탐지를 불가능하게 하고 로그 기록 등을 변조해서 시스템 복구나 침입자 추적이 불가능하게 하는 경우가 비일비재하다. 그리고, 정보보호 시스템으로 침입차단시스템과 침입 탐지 시스템이 있는데 이들 하나만으로는 침입을 차단하고 탐지하는 것은 부족한 면이 많다.

본 논문에서는 생체 면역 기반의 하이브리드 침입 탐지 시스템 설계하는데 있어서, 오용 행위 탐지 모듈에서는 잘 알려진 해킹 기법을 규칙 기반으로 시나리오화 하여 데이터 베이스에 저장한 다음, 비정상행위 탐지 모듈에서 학습한 규칙과 함께 침입을 탐지하고, 비정상행위 탐지 모듈에서는 유전자 알고리즘[6]과 Sequential Niching 알고리즘[7,8]을 통하여 새로운 규칙을 학습하여 침입을 탐지한다. 또 시스템의 로그와 같은 감사 자료와 침입을 탐지하는 시스템을 별도의 서버로 구성하여 침입을 탐지한다. 그리고 침입 차단 시스템을 침입탐지 시스템에 임베디드 하여 침입을 탐지하였다.

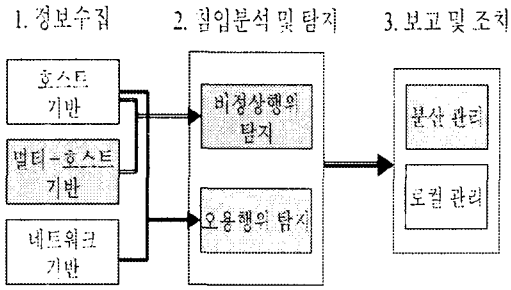
따라서, 본 논문은 부정적 결함을 비정상행위 탐지로 다시 한번 탐지할 수 있도록 하였고, 비정상행위 탐지 기법에서는 평가함수의 최소값을 사용함으로 인해 긍정적 결함을 줄이도록 노력하였다. 또, 비정상행위 탐지 기법에서 학습한 내용을 오용 행위 탐지 기법에서 사용함으로 인해 면역력이 생긴 침입에 대해 신속하게 대응할 수 있도록 하였고, 다중호스트 기반에서 하나의 시스템에서 침입을 탐지하므로 면역력이 생긴 침입을 모든 호스트에서도 면역력이 생성된다.

# 2. 관련 연구

## 2.1 침입 탐지 기법의 분류

침입 탐지 시스템은 정보수집 단계와 침입분석 및 탐지, 보고 및 조치의 단계를 거치면서 침입 판정을 하고 대응을 하게 된다[그림 1].

정보수집 단계에서는 탐지하고자 하는 대상으로 호스트 기반, 멀티호스트 기반, 네트워크 기반으로 분류할 수 있고, 침입분석 및 탐지 단계에서는 탐지 기법에 따라 오용 행위 탐지 기법과 비정상행위 탐지 기법으로 분류한다. 그리고, 보고 및 조치의 단계에서는 분산 관리와 로컬관리로서 분류할 수 있다.



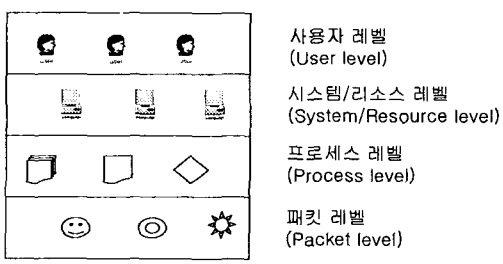

[그림 1] 침입탐지의 단계에 따른 분류

#### 2.2.1 침입 탐지 기법의 장·단점

호스트 기반의 침입 탐지 시스템은 암호화 세션에 영향을 안 받고, 실제 해킹(시도)판단에 유리하며, 네트워크 기반의 침입 탐지 시스템은 여러 유형의 침입(스캐닝, 서비스 거부 공격, 웜 바이러스 코드)을 탐지할 수 있다. 또, 오용 행위 탐지 기법에서는 잘 못된 탐지(긍정적 결함)의 가능성이 작고, 설치 즉시 사용할 수 있으며, 비정상행위 탐지 기법은 완전한 침입 탐지의 가능성이 있고, 학습 능력을 포함하고 있다. 단점으로는 호스트 기반은 침입이 이루어지는 동안 호스트의 일정 리소스를 점유하고, 네트워크 기반의 침입 탐지 시스템은 암호화 세션에 대해서는 분석이 불가능하다. 오용 행위 탐지 기법은 알려진 침입 패턴을 미리 정의하므로, 알려진 침입 패턴의 수집이 어렵고, 정의가 되어 있지 않으면 부정적 결함이 발생할 수 있다. 비정상 행위 탐지 기법은 긍정적 결함이 많이 발생할 수 있고, 장기간 학습이 필요하며 관리의 어려움이 있다.

### 2.2 정보 수집과 필터링

연결 유형과 사용자의 유형 해석에 대하여 수치적 표현이 가능할 만한 파리미터를 모니터링 한다. 시스템 로그와 ps, vmstat, netstate 등과 같은 Unix 명령어를 사용하고, 선택된 값들을 얻기 위해 결과를 필터링 한다[그림 2].

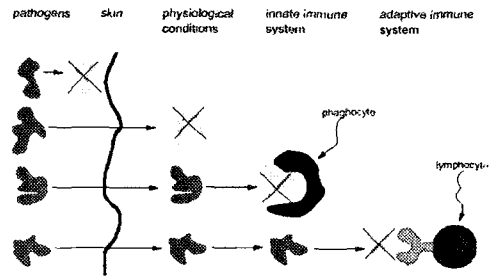



[그림 2] 다른 레벨의 파라미터 모니터링

[그림 2]와 같이 사용자 레벨, 시스템/리소스 레벨, 프로세스 레벨, 패킷 레벨의 멀티 레벨에서 정보를 수집하고 필터링 하여 감사 자료로 사용한다.

### 2.3 생체 면역 시스템

[그림 3]과 같이 생체 면역 시스템의 구조는 항원으로부터 1차적으로 피부가 보호하고 입·소화기관을 통해 피부를 통과한 항원은 물리적인 조건에 의해서 자연 소멸된다.




[그림 3] 생체 면역 시스템

물리적 조건에 의해 자연 소멸되지 않은 항원과 입·소화기관을 통과하지 않고 직접 피부를 통해 침입한 항원이 맞이하게 되는 면역은 선천성 면역이다. 선천성 면역은 항원에 대하여 면역력이 생성된 것이고 항원에 대해 신속하고 정확하게 대응하여 항원을 분해 처리하게 된다.

아직 면역력이 생성되지 않은 항원에 대하여 림프구는 항원에 적응하면서 면역력을 생성하여 항원으로부터 방어하게 된다.

#### 2.3.1 선천성 면역

최후의 방어선인 피부가 부상했다고 가정해 보자. 그곳에는 많은 미생물들이 침범할 것이며 이들은 곧 몸의 2차 방어선인 선천성 면역을 공격할 것이다. 공격을 받게 되면, 처음 몇 일간 감염을 저지하는 염증으로 대응하는데, 때로는 이 대응이 아주 효과적이어서 더 이상의 반응이

필요 없을 수도 있다. 선천성 면역 반응의 중요성은 그 미생물들이 무해한지 유해한지를 재빨리 구별하는 점이다.

#### 2.3.1 후천성 면역

미생물들은 상당히 빨리 진화하고 그보다 다소 느리게 진화하는 인간과는 다른 종들의 면역 방어 능력을 공격할 수 있는 가능성을 가졌기 때문이다. 미생물이 만약 침투에 성공했다면 세 번째, 즉 마지막 방어선인 획득 또는 후천성 면역반응능력을 공격하게 된다. 후천성 면역 에 대하여 인체는 어떤 침범자「이전에 한번도 감염된 적이 없는 경우에도」에 대하여 복잡 미묘하고 모양에 걸맞은 방법으로 인식하여 특이적으로 반응한다. 후천성 면역 반응의 중요성은 항원 수용체는 전 우주에 산재해 있는 거대한 스케일의 모든 침입자들을 구분하여 대처하는 능력을 가지고 있다.

## 3. 생체 면역 기반의 하이브리드 침입 탐지 시스템

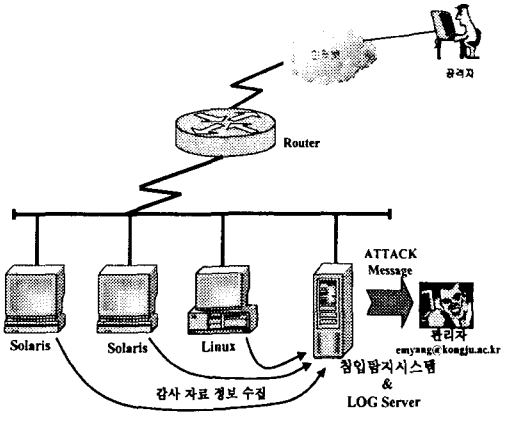
### 3.1 시스템 특징

본 시스템 특징으로는 외부에서 침입한 병원균을 효과적으로 탐지 및 파괴하는 인체 면역 시스템을 응용하려는 면역 메커니즘 기반의 침입 탐지시스템이다. 오용 행위 탐지 기법에서는 비정상행위 탐지 기법의 단점인 잘 알려진 버그와 해킹기법에 대한 대응이 부족한 것을 보완하고, 비정상행위 탐지 기법에서는 오용 행위 탐지 기법의 단점인 부정적 결함과 유사한 침입에 대한 학습과 대응이 미비한 것을 보완한다. 그리고, 방화벽 기능을 하는 서비스 제한 에이젠트를 두어 꼭 필요한 서비스만 서비스 되도록 하여 시스템에 악영향을 미칠 수 있는 불필요한 해킹 시도를 원천적으로 봉쇄하였다. 또 서비스 제한 에이젠트는 특정 서비스만 서비스하도록 허가받아서 특정 서비스의 감사 자료를 수집할 수 있도록 하며, 효과적인 대응을 하기 위해서 서비스 제한 에이젠트를 사용할 수 있다. 마지막으로, 비정상 행위 탐지에서 규칙 기반의 학습하여 오용 행위 탐지기법에 적용하는 단일 시스템의 면역뿐만 아니라, 탐지 대상이 되는 다중호스트 전체의 면역력을 향상시키고, 각 레벨에서 수집된 파라미터를 평가함에 있어서 평가의 높은 값은 더 강한 대응을 하기 때문에 각 레벨에서 수집된 파라미터의 값을 최저 가치로 평가하므로 인해 긍정적 결함을 줄였다.

### 3.2 시스템의 구조

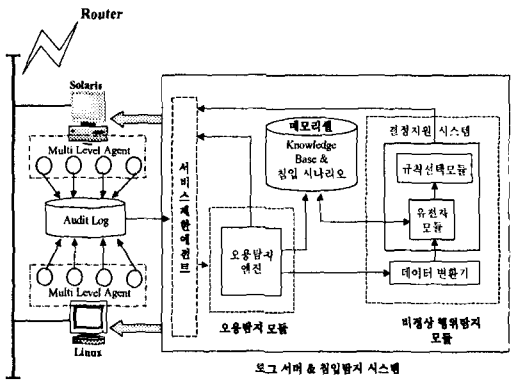
[그림 4] 의 네트워크 구성도와 같이 Solaris와 Linux를 침입탐지 대상으로 하고, 실시간으로 멀티레벨 파라미터의 감사자료가 침입탐지 시스템 및 로그서버에 저장된다.

침입 탐지와 침입자 추적에 중요한 단서를 제공해 주는 로그 기록을 별도의 서버를 제공함으로 시스템이 침입을 당했을 때 해커에 의해 로그기록이 삭제되는 것을 방지하고, 로그 기록을




[그림 4] 침입 탐지 시스템의 네트워크 구성도

통한 침입자 추적을 가능하게 한다. 그리고, 다중 호스트로부터 사용자 레벨과 다른 레벨에서 감사 자료를 한 곳에 모음으로써, 개별적인 감사 자료 분석을 통한 침입 탐지에서 찾을 수 없는 공격 형태도 탐지할 수 있다




[그림 5] 침입 탐지 시스템의 구조

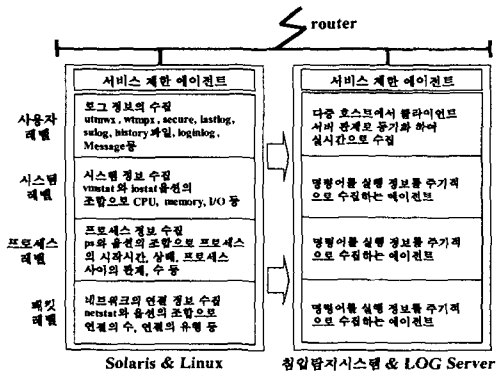
본 논문에서 제안한 시스템의 전체적인 구조는 [그림 5]와 같다. 본 시스템의 구성요소는 크게 3개의 모듈(감사자료 수집 모듈, 오용 탐지 모듈, 비정상 행위 탐지 모듈)과 그 외의 부분으로 구성된다.

감사자료 수집 모듈은 멀티 레벨에서 침입을 탐지하기 위해 필요한 파라미터 정보들을 수집하고 필터링 하는 역할을 담당한다. 이때 서비스 제한 에이전트는 특정 서비스만 허가하므로 허가된 특정 서비스의 감사자료가 수집된다. 오용 탐지 모듈은 감사자료로 수집된 멀티레벨 파라미터들을 면역 메모리에 미리 저장된 시나리오를 비교하여 침입을 판정하게 된다. 비정상 행위 탐지 모듈은 감사자료를 바이너리 스트링으로 변환하는 데이터 변환기와 변환된 바이너리 스트링을 입력으로 유전자 규칙 생성 모듈(Genetic Rule Generation Module)을 이용하여 규칙 기반의 베스트 규칙을 찾아낸다. 그리고, 규칙 선택 모듈(Rule Selection Module)에서는 최적의 대응 규칙을 찾아 대응하게 된다.

### 3.3 시스템의 구성 요소

#### 3.3.1 감사 자료 수집 모듈

[그림 6]은 침입 탐지 대상이 되는 시스템의 감사 자료를 실시간으로 수집하는 에이전트에 대한 그림이다.




[그림 6] 감사 자료 수집 모듈

감사 자료 수집 모듈은 침입 판정에 필요한 정보를 수집하고 필터링 하는 모듈이다. Unix시스템이라 해도 운영체제 종류에 따라 다른 형태의 감사 자료를 제공한다. 그러므로, 운영체제 종류에 따라서 감사 자료를 실시간으로 LOG Server로 보낼 수 있는 에이전트를 두어 감사 자료를 수집한다. 본 논문에서는 Solaris와 Linux를 그 대상으로 한다.

침입 탐지 대상이 되는 시스템은 특정 서비스만 허가하는 서비스 제한 에이전트가 있고, 서비스 제한 에이전트는 침입으로 판정되었을 경우, 특별한 IP주소를 차단하거나, 원격 접속을 허용하지 않는 방법으로 대응할 수 있다.

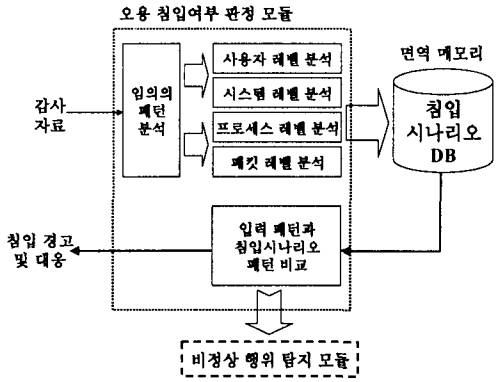
#### 3.3.2 오용탐지 모듈

[그림 7]는 오용행위 탐지 모듈에 대한 간단한 구조와 흐름도 이다.

감사 자료로 입력되는 임의의 패턴을 분석하여 침입 시나리오 DB와 비교하여 침입 시나리

오에 패턴이 존재하면 침입 경고 및 대응이 이루어지고, 침입 시나리오 패턴이 존재하지 않으면, 계속해서 비정상 행위 탐지가 이루어진다.

오용 행위 탐지 모듈에서는 감사 자료로 수집된 임의의 패턴 분석이 이루어진다. 이 패턴 분석은 사용자 레벨과 시스템 레벨, 프로세스 레벨, 패킷 레벨에서 분석이 이루어진다. 분석이 이루어진 패턴은 침입의 시나리오와 비교를 하는데 여기 에서는 분석되어진 패턴이 「침입 유형(공격 행위)과 일치하는가?」를 비교하게 된다. 그래서, 비교되어진 패턴이 침입 시나리오에 존재하면, 침입 경고 및 대응이 이루어지고 침입 패턴이 존재하지 않으면 계속해서 비정상 행위 탐지로 넘어 가게 된다. 오용 행위 탐지 모듈에서는 침입 시나리오가 DB형태로 존재하므로 언제든지 관리자가 새로운 패턴을 정의해서 내장해서 새로운 버그나 해킹 기법에는 신속하게 대응할 수 있다. 또한 비정상 행위 탐지 모듈에서 침입 행위로 탐지한 규칙은 오용행위 탐지 모듈의 시나리오에 추가되어 침입 탐지 시스템의 면역력을 향상시킨다.



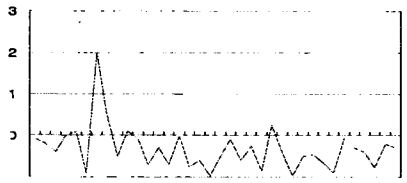

[그림 7] 오용 행위 탐지 모듈에 대한 구조와 흐름

3.3.3 비정상 행위 탐지 모듈

비정상 행위 탐지 모듈에는 오용 행위 탐지 모듈에서 탐지하지 못한 부정적 결함과 정상 사용 패턴이 비정상 행위 탐지 모듈의 입력으로 들어온다.

3.3.3.1 데이터 변환기

데이터 변환기에서는 비정상 행위 탐지 모듈의 입력으로 들어온 것을 [그림 8]와 같이 그래프로 변환한다.




[그림 8] 침입 정도에 따른 그래프 변환

그래프에 의해 변환된 감사 자료를 <표 1>과 같이 침입의 정도에 따라 (0~3)로 표시하는 2비트 문자열로 변환한다. 00은 정상적인 상태이고, 01은 약간의 침입 징후가 보이는 것이고, 10은 침입의 상당히 많은 곳에서 침입의 징후가 표시되는 것이고, 10은 아주 위험한 상황이어서 침입이라고 간주할 수 있다.

<표 1> 파라미터 값의 바이너리 인코딩

| | | |
|---|---|---|
| 0 | 00 | Normal |
| 1 | 01 | Minimal |
| 2 | 10 | Significant |
| 3 | 11 | Dangerous |

3.3.3.2 분류자 시스템(Classifier System)을 이용한 학습

학습의 과정은 조건과 선택으로 된 고정길이 문자열로 유전자 알고리즘의 선택의 방법을 진화 시켜 환경에 대처하기 위한 적응형 학습 시스템이다.

<표 2> 서로 다른 레벨들에서 침입한 활동에 대한 평가들과 반응작용의 예

| 가설 | 유저 레벨 | 시스템 레벨 | 프로세스 레벨 | 패킷 레벨 | 반응 |
|---|---|---|---|---|---|
| 1 | 0.2 | 0.0 | 0.0 | 0.1 | 1 |
| 2 | 0.4 | 0.0 | 0.0 | 0.4 | 3 |
| 3 | 0.0 | 0.1 | 0.2 | 0.8 | 6 |

보안정책과 전문가들에 의해 생성된 지식베이스를 바탕으로 학습에 사용될 규칙을 정의한다. 이것은 조건(0~3)과 공격 유형에 따라서 명확한 대응(0~7)으로 표현한다. 일반적인 규칙을 만들고, 그러한 지식베이스는 <표 2>와 같이 대응의 높은 값은 조금 더 강한 대응을 한다.

상징적으로, 각 가설은 5개의 튜플(Tuple)(k1, k2, k3, k4, a)로 구성되고, ki∈ [0.0, 1.0]이고 a ∈{0,...,7}의 대응 값을 나타낸다. [그림 9]의 분류에 근거한 결정지원 시스템에 있는 메시지리스트(m1, m2, m3, m4)에 포함된다. 이 가설이 메시지들과 일치한다고 생각하면,

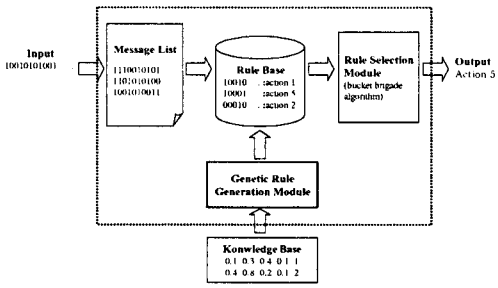
$$k1 \leq m1,\ k2 \leq m2,\ k3 \leq <= m3,\ k4 \leq m4$$

와 같이 나타낼 수 있다. 이것은 가설의 조건부분은 서로 다른 레벨에서 침입 정도의 최저 가치를 나타낸다.

따라서, 가설 K = (k1, k2, k3, k4, ak), 가설 L = (l1, l2, l3, l4, la)이 있고(i = 1, 2, 3, 4), ki < li 라고 가정하면, 가설 L은 가설 K보다 더 명확한 가설이고, 지식 베이스의 일관성을 유지하게 위하여 가설 L의 대응값(al) 가설 K의 대응값(ak) 보다 더 강한 대응을 한다. 이러한 특징은 지식베이스의 강건함을 증가시킨다.

3.3.3.3 유전자 알고리즘 모듈

멀티 레벨에서 모니터링된 파라미터 값들의 상호 관계로 액션 값을 결정하게 된다. 데이터 변환기에서 변환된 바이너리 스트링은 유전자 알고리즘 모듈에서 대응되는 값을 찾기 위해 메시지 리스트에 놓이게 된다. 만약 대응되는 값이 없으면 유전학적인 연산을 통해 진화 시켜 새로운 대응 값을 찾게 된다.




[그림 9] 분류에 근거한 결정 지원 시스템

[그림 9]은 데이터 변환기에서 바이너리 스트링으로 변환된 것을 입력으로 하는 분류에 근거한 결정 지원 시스템으로, 입력에서 일정 프레임의 범위를 잡고, 유전자 알고리즘으로 추출한 최적의 규칙 값과 비교하는 규칙 선택 모듈(Rule Selection Module)을 통해서 최적의 반응 값을 찾아낸다.

분류 규칙은 다음과 같은 서식을 가지고 있다.

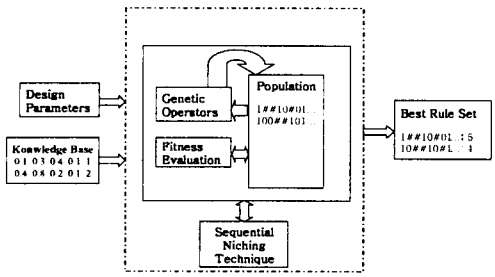
<condition> : <action>

조건부분(<condition>)의 바이너리 스트링은 {'0', '1', '#'}으로 되어 있고, '#'은 '0'과 '1'에 대응될 수 있는 don't care 조건이다. 대응 값(<action>)은 침입 정도에 따라 8가지 대응 값으로 대응할 수 있다.

[그림 9]은 분류에 근거한 결정 지원 시스템에서 제안된 유전자 알고리즘을 적용한 일반적인 모듈이다. 이로서 후천성 면역인 비정상 행위를 탐지는 감사자료 수집과 필터링이 이루어진 후 선천성 면역인 오용행위 탐지 기법에서 탐지하지 못한 부정적 결함과 정상 행위를 바이너리 스트링으로 변환, 유전자 알고리즘을 이용한 학습과 적응의 단계를 거치면서 탐지 율을 높이게 된다. 또 적합도 평가를 통해 학습의 강

도를 조정할 수 있다.

[그림 9]에서 보이는 규칙 선택 부분(Rule Selection Module)은 [그림 10]에서 생성한 베스트 규칙 중에서 대응할 규칙을 선택하는 부분이다. 서열 비교평가를 통해 새로운 규칙을 찾아내고 진화시켜 새로운 규칙을 생성한다.




[그림 10] 규칙에 근거한 일반적인 유전자 알고리즘 모듈

3.3.3.4 적합도 평가 함수

평가 함수의 목적은 문제해결에 각 염색체가 얼마나 좋은가는 측정하는 것이다. 제안한 접근 중에서 규칙 집합을 만드는 동안 다음의 요소들을 고려한다.

- 규칙에 전문가의 지식 베이스를 얼마나 잘 반영하는가?
- 규칙의 일반적인 수준
- best 규칙 집합의 다양성

평가함수의 기능을 설명하기 위하여, 염색체를 C =<c1,c2, ... , c40>로 표현할 수 있다, ci ∈ {'0','1','#'}로 구성되고, 염색체(c)는 아래 구조의 일부분으로 표현된다<표 3>.

<표 3> 변환된 바이너리 스트링

| $P^1$ | ... | $P^4$ |
|---|---|---|
| $P^1_1$ ··· $P^1_5$ | ... | $P^4_1$ ··· $P^4_5$ |
| $c_1c_2$ ... $c_9c_{10}$ | ... | $c_{31}c_{32}$ ... $c_{39}c_{40}$ |

Pi 는 감사자료의 레벨을 나타내고(i=1 user, i=2 system, i=3 process, i=4 packet), Pij 는 염색체의 파라미터를 나타낸다(i = 1,...,4).

평가함수의 정의를 위해서 다음과 같은 정의가 필요하다.

Min(Pij) : Pij의 최소 값은 <표 4>와 같이 정의할 수 있다.

<표 4>바이너리 스트링에 대한 최소값

| $P^i_i$ | $Min(P^i_i)$ |
|---|---|
| 00 | 0 |
| 01 | 1 |
| 10 | 2 |
| 11 | 3 |
| 0# | 0 |
| #0 | 0 |
| 1# | 2 |
| #1 | 1 |
| ## | 0 |

따라서

$$MinValue(P^i) = \frac{1}{5}\sum_{j=1}^{5}\frac{Min(P^i_j)}{3} \qquad (1)$$

NumWC(Pi) : Pi 에서 '#' 문자의 수로 나타내고, 데이터 변환기에서 이야기되었던, 가설(k1,k2,k3,k4,a)의 실제 값에 의해 표현된다. 그리고, knowledgeDist 함수는 지식베이스에 의한 하나의 명확한 규칙을 만들기 위해 각 레벨에서 최소 값으로부터 거리가 정의된다. 여기서 최소값을 사용하는 것은 비정상 행위의 잘못된 탐지 즉, 긍정적 결함(False Positive)을 줄이고자 하는 이유이다.

$$KnowledgeDist(C) = \frac{1}{4}\sum_{i=1}^{4} |K_i - MinValue(P^i)| \quad (2)$$

Generality의 함수의 의미는 wildcards('#')의 최적의 개수와 각 레벨의 개수와 비교해서 개수의 차이를 의미한다. 여기서, GenCoef의 값은 0.0에서 1.0의 값을 가지며, 평가함수의 일반적인 중요성을 조건으로 지정하였다.

$$Generality(C) = GenCoef * \frac{1}{4}\sum_{i=1}^{4} | OptNumWC - NumWC(P^i) | \quad (3)$$

적합도는 2에서 KnowledgeDist와 Generality를 빼는 것으로 계산되며, 이후로 적합도의 최대 값은 2.0으로 구성된다.

$$Fitness(C)=2-KnowledgeDist(C)-Generality(C) \quad (4)$$

다양한 규칙을 만들기 위하여 Sequentail Niching Algorithm(SNA)을 사용한다. SNA는 평가 함수를 사용하기 위해 거리 매트리스(distance metric)가 필요하다. 다음에 설명된 평가 함수의 기능을 수정하여 GA 모듈에 반복하여 실행한다.

유전자 알고리즘을 실행하기 이전의 베스트 규칙을 B = <b1, b2, ..., bn>이라고 하자, SNA는 베스트 규칙을 만들기 위하여 규칙의 평가 값은 규칙의 거리 값에 의존한다. 규칙 f가 있을 때, 규칙 f와 베스트규칙 bi사이의 거리를 dist(f,bi)라고 하면, 수정된 평가 함수 f(fitness'(f))의 정의 다음과 같다.

$$fitness'(f) = M_n(f) \quad (5)$$

여기서,

Mo = Fitness(f)

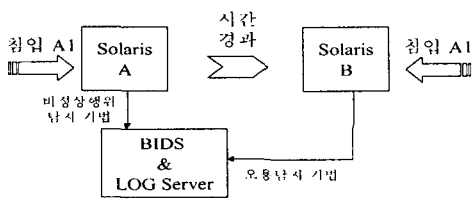
Mn+1 = Mn * G(f, bi)

$$G(f, b_i) = \begin{cases} (dist(f, b_i) / R)^{\alpha} & if\ dist(f, b_i) < R \\ 1 & otherwise \end{cases} \quad (6)$$

$\alpha$와 R은 Sequential Niching 알고리즘의 파라미터이다.

3.3.3.5 새로운 침입에 면역 반응

본 논문에서 제안한 시스템은 새로운 침입에 대해 첫 번째로 A 호스트에서 A1이라는 침입을 탐지하였을 경우 A1이라는 침입에 대한 면역 항체가 생성되었다. 그래서 시간이 경과한 다음 B라는 시스템에 A1라는 침입이 이루어졌을 경우 이를 신속하게 탐지하고 대응하게 된다. A라는 호스트에서 오용탐지 기법으로 탐지 못한 침입에 대해 비정상 행위탐지 기법에서 탐지를 하여 적응해서 규칙 기반의 시나리오가 오용 행위 탐지 기법의 면역 메모리에 추가되어 다음에 같은 침입이 이루어지면 오용탐지 기법에서 신속하게 탐지하고 대응하게 된다.[그림 11]




[그림 11] 새로운 침입에 대한 면역력 향상

## 4. 실험 및 평가

분류에 근거한 결정 지원 시스템을 평가하기 위하여, 분류자 시스템을 이용한 학습을 근거로 하여 다음과 같은 가정을 만들었다.

1. If U>=0.2 or S>=0.2 or P>=0.2 or N>=0.2 then execute Action 0.
2. If N>=0.5 or U>=0.5 or P>=0.5 then execute Action 1.
3. If (U>=0.4 and S>=0.2) or (P>=0.4 and N>=0.4) then execute Action 2.
4. If U>=0.8 or S>=0.8 or P>=0.8 or N>=0.8 then execute Action 3.
5. If (U>=0.4 and P>=0.6) or (S>=0.4 and N>=0.6) then execute Action 4.
6. If (U>=0.5 and S>=0.6) or (P>=0.5 and N>=0.6) then execute Action 5.
7. If (U>=0.6 and S>=0.2 and P>=0.6) and (N>=0.6 and P>=0.6) then execute Action 6.
8. If U>=0.7 and S>=0.7 and P>=0.7 and N>=0.7 then execute Action 7.

위에 가정들을 가지고 분류 규칙을 생성하는 것으로 실험하였다. 처음부터 4번째의 가정으로 위의 적합도 평가 함수에 보이는 예제와 같이 40-bit messages를 임의로 만들어서 사용하였다. 실험의 목적은 임의의 어떤 패턴으로부터 규칙을 진화시키고 성능을 테스트하는 것이다. 실험의 결과를 가정에 대한 대응 값과 출력에 대한 연결 대응 값을 비교하였다.

<표 5> 분류에 근거한 결정 지원 시스템의 실험 결과

| 가설 / 연결 대응 | 분류에 근거한 결정 지원 시스템 출력 | | | |
|---|---|---|---|---|
| 연결 대응 | 1 | 2 | 3 | 4 |
| 1 | 78% | 22% | 0% | 1% |
| 2 | 2% | 96% | 0% | 2% |
| 3 | 7% | 38% | 53% | 3% |
| 4 | 0% | 4% | 17% | 79% |

<표 5>에서 보듯이, 연결 대응 1을 보면, 가설의 대응이 1일 때 연결 대응은 78%로 나타나고 가설에서 대응 2일 때, 연결대응이 1인 것은 22%로 나타나고 가설의 대응이 3일 때 연결대응이 0%, 가설 대응이 4일 때는 연결대응이 1%로 나타났다.

위의 실험의 결과로 다음과 같은 규칙을 생성할 수 있다.

만약 연결이 외부 연결이고 CPU사용량이 임계값보다 크고 사용 가능 메모리가 매우 적고 swap이 최소이면 Action A4로 대응하고, 만약 연결이 외부 연결이고 받는 패킷의 평균량이 임계값보다 크고 연결이 지속 시간이 임계값보다 크면 Action A6으로 대응하고, 만약 연결 수가 임계값보다 크고 실행중인 프로세스가 임계값보다 크고 swap의 양이 최소이면 Action A5로 대응을 하며, 만약 연결이 내부 연결이고 CPU 사용량이 임계값보다 크고 메모리 사용량이 임계값보다 크고 보내고 받는 패킷의 양이 임계값보다 크면 즉시 Action A1으로서 대응을 하게 된다. 그리고, 만약 CPU 사용량이 임계값보다 크고 메모리 사용량이 임계값보다 크고, 프로세스의 권한에 의해 막힌 수가 임계값보다 크면 Action A2로 대응한다와 같은 결과의 규칙을 생성할 수 있다.

## 5. 결 론

인터넷과 네트워크의 대규모화로 모든 컴퓨터가 연결되어 많은 편리한 기능을 제공하지만, 그에 따른 역기능도 무시 못하는 것이 현실이다.

본 논문은 침입 탐지 시스템 & 로그서버를 탐지 대상이 되는 시스템과 분리하였다. 별도의 서버로 침입 탐지 시스템과 로그 서버를 구성하는 것은 침입이 이루어졌을 경우 해커에 의한 로그 기록의 변조를 막고, 로그에 의해 해커를 추적하는 데 사용할 수 있다. 또, 탐지 대상이

되는 시스템과 침입을 탐지하는 시스템을 분리함으로 인해 탐지가 이루어지는 동안 탐지 대상 시스템의 일정 리소스를 점유한다는 단점을 보안하였다. 오용 행위 탐지 기법의 단점인 부정적 결함을 비정상 행위 탐지 기법으로 탐지할 수 있고, 비정상행위 탐지 기법의 단점인 긍정적 결함은 평가 함수를 최저 가치로 표현함으로 인해 긍정적 결함을 감소 시켰으며, 하나의 호스트에서 탐지된 침입은 다른 호스트에 같은 침입이 들어오면 이미 그 침입에 유형에 관해서는 학습이 이루어 졌으므로 쉽게 침입을 판단할 수 있는 면역력을 가지고 있다.

향후 연구 방향은 비정상 행위 탐지 기법에서 전문가적인 지식이 필요한 가정에 대한 행동 값의 정의에 관한 연구가 필요하다.

## 참고문헌


[1] 양은목, 이상용, "생체 면역을 이용한 하이브리드 침입탐지 시스템의 설계," Proceedings of the 16th KIPS Fall Conference Vol.8, No.2 pp. 523 - 526, 2001.

[2] Balasubramaniayn J.S, Garcia-Fernandez J.O, Spafford E, Zamboni D, "An Architecture for Intrusion Detection using autonomous Agents," Technical Report 98-05, COAST Laboratory, Purdue University, May 1998.

[3] Base R, Mel P, "NIST Special Publication on Intrusion Detection System," Computer Security Center(CSD), SP 800-31, August 2001.

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

[5] Dasgupta D, "Immunity-Based Intrusion Detection Systems: A General Framework", In the proceedings of the 22nd National Information Systems Security Conference (NISSC), October 18-21, 1999.

[6] Jeffrey, Kephart O, "A Biologically Inspired Immune System for Computer," Artificial Life IV, R. Brooks and P. maes, eds., MIT Press, 1994.

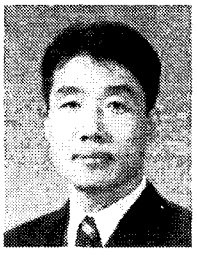
[7] Mahfoud S. W, "A Comparison of Parallel and Sequential Niching Methods," Proceedings of the Sixth International Conference on Genetic Algorithms, 136 - 143, 1995.

[8] Sandeep K, "Classification and Detection of Computer Intrusions", Ph.D Thesis, Purdue University, August 1995.



**양 은 목**

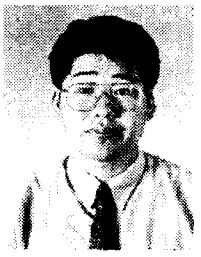
2000년 한밭대학교 전자계산학과 졸업(학사)
2002년 공주대학교 전자계산학과 졸업(이학 석사)
2002년 현재 공주대학교 전자계산학과 박사 과정
관심분야: 기계학습, 에이전트시스템, 시스템 보안등



**이 상 용**

1984년 중앙대학교 전자계산학과 졸업 (학사)
1988년 일본동경공업대학 시스템과학 졸업(공학 수사)
1993년 중앙대학교 일반대학원 전자계산학과(공학 박사)

1988년-1989년 일본전기(주) 중앙연구소 연구원
1993년 - 현재 공주대학교 정보통신공학부(인공지능 전공) 교수
1996년 - 1997년 미국 University of Central Florida(교환교수)
관심분야: 인공지능, 기계학습, 에이전트 시스템



## 서 창 호

1990년 고려대학교 수학과 졸업(학사)
1992년 고려대학교 일반대학원 수학과(이학석사)
1996년 고려대학교 일반대학원 수학과(이학박사)
1996년-1996년 국방과학연구소 선임연구원
1996년-2000년 한국전자통신연구원 선임연구원, 팀장
2000년 - 현재 공주대학교 응용수학과(정보보호 전공) 조교수
관심분야: 암호 알고리즘, PKI, 무선 인터넷 보안,시스템 보안 등

## 김 석 우

1979년 한국항공대학교 통신정보공학과(학사)
1989년 뉴저지 공과대학 전자계산학과(공학석사)
1995년 아주대학교 컴퓨터공학과 정보통신전공(공학박사)
1980년 - 1997년 한국전자통신연구원 책임연구원, 실장
1997년 - 현재 한세대학교 IT학부/대학원 정보보호공학과 교수
관심분야: 시스템 보안, 네트워크 보안, 시스템 평가 등