네트워크 침입 탐지를 위한 인공 면역 모델의 개발[1)]

김정원* · Peter Brently** · 정길호*** · 최종욱****

A Development of Artificial Immune Model for Network Intrusion Detection

Jungwon Kim*, Peter Brently **, Gilho Jung***, JongUk Choi****

요 약

This paper investigates the subject of intrusion detection over networks. Existing network-based IDS's are categorised into three groups and the overall architecture of each group is summarised and assessed. A new methodology to this problem is then presented, which is inspired by the human immune system and based on a novel artificial immune model. The architecture of the model is presented and its characteristics are compared with the requirements of network-based IDS's. The paper concludes that this new approach shows considerable promise for future network-based IDS's.

Key words: 인공면역체계(Artificial Immune System), 네트워크 침입 탐지(Network Intrusion Detection), 진화 알고리즘(Evolutionary Algorithm), 컴퓨터 보안(Computer Security)

1. 소개문

침입탐지시스템(Intrusion Detection System)은 컴퓨터 시스템에 대한 침입을 탐지하는 자동화 시스템이다. 이전의 침입탐지시스템들은 호스트 수준에서의 작업을 수행하였으며 최근에는 이러한 시스템들이 네트워크 기반으로 되고 있는 경향을 보이고 있다 [5]. 호스트기반의 침입탐지시스템은 단지 호스트의 운영체제로부터 얻어진 감사증적(audit trail)을 이용하여 단일 호스트기계에 대한 감시를 수행하며 네트워크 기반의 IDS는 다중 호스트들의 감사증적을 점사해 네트워크 상에서의 호스트들의 집단을 감시한다. 이외에도 다양한 접근법이 개발되거나 제안되고 있으나 네트워크기반의 IDS들이 모든 침입탐지 시스템에 대한 요구사항들을 만족시키지는 못하고 있다.

본 논문에서는 인간 면역 체계에서 고안된 네트워크 기반의 IDS를 구축하기 위한 새로운 접근법을 제안한다. 그리고 더 자세히 인공면역모델에 대한 특징을 소개하고 본론으로 들어가 실제 네트워크 상에서의 감시와 이러한 모델의 주요 구성요소들에 대해 언급할 것이다.

본 논문은 다음과 같은 내용을 다룬다: 2절은 기존에 존재하는 네트워크 기반의 침입탐지시스템을 3가지 형태로 분류하며 각각의 접근법과 각 접근법의 한계에 대하여 요약하였다. 3절에서는 인공면역 모델을 이용한 새로운 네트워크 기반 IDS의 구조를 소개한다. 이 시스템의 특징은 4절에서 네트워크 기반의 IDS들에 대한 요구사항들을 가지고 비교 분석한다. 그리고 논문의 마지막에서는 본 논문에서 나온 결과를 바탕으로 한 결론부분으로 되어 있다.

2. 네트워크 기반 침입탐지시스템의 분류

전체적인 구조에 따라 우리는 네트워크 기반의 침입탐지시스템을 단일구조, 계층적구조 그리고 상호협동적구조.로 분류한다.

2.1 단일구조 접근법(monolithic approach)

단일 구조 접근법은 중앙에 하나의 침입탐지 서버를 설치하는 것으로 다중 로컬 호스트를 기반으로 하는 간단한 호스트 감사(audit) 프로그램을 돌리는 것이다. 감시대상인 로컬 호스트들은 침입

1) 본 작업은 부분적으로 과학기술부 국제공동연구과제(I-03-002)의 지원에 의해 수행되었슴.

* Universe college of London
** Universe college of London
*** 상명대 정보통신학부
**** 상명대학교 정보통신학부

탐지서버에게 그들이 수집한 감사증적(audit trail)을 전송하며 전송 받은 서버는 감사증적에 대한 분석을 수행한다. 대부분의 네트워크 기반 침입탐지시스템은 현재 이러한 접근법을 사용하여 개발되어진 것들이며 실제로 작은 규모의 네트워크 상에서 실행 된다. 이러한 단일 구조 방법은 scalability, robustness 그리고 configurability에 대한 문제점을 지고 있다. 첫 번째, 네트워크 크기가 증가함에 따라 감사증적의 거대한 수가 로컬 호스트로부터 중앙 서버로의 전송을 필요로 하게 된다. 이러한 이유 때문에 네트워크 성능의 급속한 저하를 초래하였으며 또 이 접근방법은 규모성(scalability)을 보장하는 것이 어렵다. 두 번째는, 만약 중앙 침입탐지서버가 파괴되거나 실패할 경우 전체의 침입탐지시스템은 작동불능의 상태가 된다. 세 번째로는 단일의 침입 탐지 서버는 각각의 호스트들의 다양한 지역적 요구에 대해 항상 동일한 구조만을 가지며 이는 각각의 local Area에 대한 적용을 어렵게 한다.

2.2 계층구조 접근법(hierarchical approach)

계층구조 접근법은 단일 구조 접근법의 문제를 해결하기 위해 제안되었다. 이 접근법은 수천 개 이상의 호스트들을 갖는 거대한 규모의 네트워크를 감시하기 위하여 설계되었다. 로컬 호스트에서 수집되어진 모든 감사증적(audit trail)을 중앙의 IDS에 전송하는 대신에 지역을 감시하는 레벨의 단일 IDS들은 자신이 담당하는 로컬 시스템을 분석하고 로컬에 대한 분석 결과를 상위 레벨의 IDS에게 계층적으로 전달한다. 그러므로, 더 높은 계층의 IDS는 단지 전송 받은 지역 보고만을 분석하게 된다. GrIDS(Graph-based Intrusion Detection system)[9] 와 EMERALD(Event Monitoring Enabling Responses to Anomalous Live Disturbances)[7] 프로젝트는 큰 규모의 네트워크를 감시하기 위하여 이러한 접근법을 제시하였으며 현재 개발 진행중이다. 계층구조 접근법은 분산된 로컬 감시 지역에서 로컬 분석을 허용함으로써 규모에 있어 더 나은 면을 보여준다. 그러나, 단일 구조 접근법에서 나타난 문제점들이 전부 해결된 것은 아니다. 현재 네트워크의 형태가 변경되었을 때, 네트워크가 계층적으로 변화되는 것이므로 로컬 분석 보고를 모으기 위한 전체구조가 변경되어야 한다 [5]. 게다가, 가장 높은 레벨에 존재하는 감시자가 공격 당하거나 무너지면 모든 네트워크 전체 시스템의 동등한 침입이 가능하므로 침입자가 탐지를 빠져나가는 것이 더 용이 해진다.

2.3 상호 협력 구조 접근법(Co-operative approach)

상호 협력 구조 접근법은 상호 협력이 가능한 호스트기반 IDS의 집단에게 단일 중앙 서버의 책임을 분산시키기 위한 시도를 한다. 각각의 IDS는 단지 로컬 호스트의 작은 면만을 감시하는 책임을 가지며 IDS의 구성원들은 동시수행을 하거나 각각 다른 IDS와 상호 협력을 한다. 더욱이, 이들은 융통성이 강한 유형이나 전체 결점을 만들을 낼 수도 있다. 이 접근법이 계층적 구조 접근법과 다른 것은 분산된 로컬 IDS가 서로 계층적이지 않다는 것이다. 그러므로 어떠한 IDS의 실패나 파괴가 항상 동등한 공격에 대한 탐지를 방해하지는 못한다. CSM(Co-operative Security Managers)[11] 프로젝트와 AAFID(Autonomous Agent For Intrusion Detection)[1] 프로젝트는 이러한 접근법을 제안하였다. 이러한 제안은 앞에서 언급한 두 가지 접근법에서 발생된 문제점들을 해결하기 위해 강조된다. AAFID와 CSM 프로젝트는 현재 개발 진행중이며 이러한 주장이 실질적으로 증명되지는 않은 상태이다. 특히, 이러한 제안은 효율성에 있어서 다른 문제점을 초래하였다. 로컬 호스트들을 감시하는데 필요한 다량의 통신 장치나 감사 장치 그리고 감사증적의 분석과 같은 것들이 너무 많은 과부하(overhead)를 발생시키며 이러한 것은 네트워크로 하여금 중요한 결함이 될 수 있다.

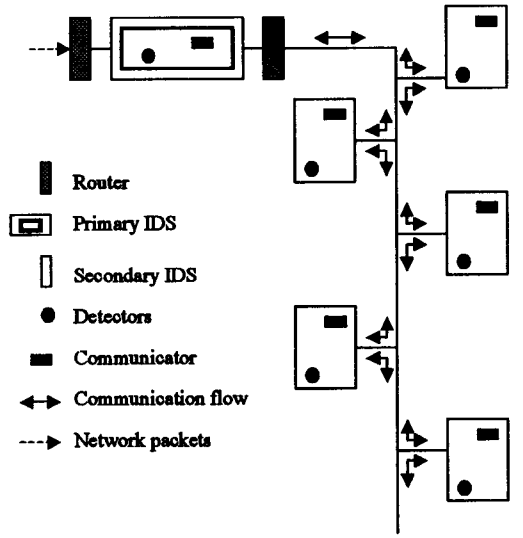
요약해 보면, 네트워크 기반 IDS에 대한 다양한 구조들이 제안되고 있으며 본 논문에서는 세 가지 다른 접근법으로 분류되었다. 각각의 접근법은 서로 다른 문제점을 보이고 있으며 직면된 문제점들을 완벽하게 해결하기 위한 네트워크 기반의 모델은 아직 개발되지 않은 상태이다.

3. 인공 면역 모델의 개요

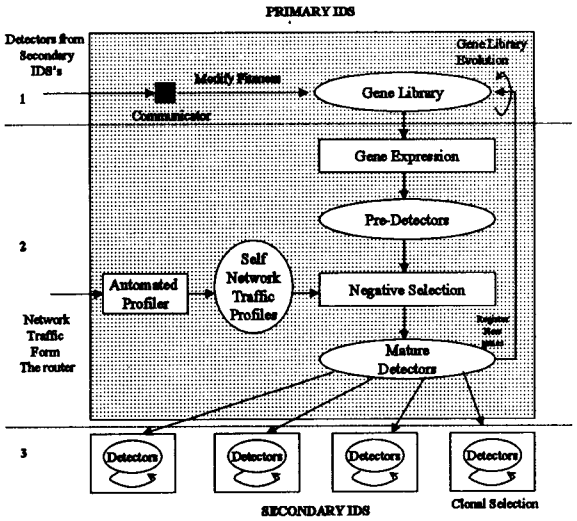
인간 면역 체계는 외부 병원체나 조직의 다양한 종으로부터 인간의 몸을 보호하는데 매우 성공적이다[10]. 이러한 두드러진 특성은 컴퓨터 보안 연구자들이나 인공지능 연구자에게는 매혹적인 분야라 할 수 있다. 면역학에 기반을 두고 다수의 다른 컴퓨터 면역 모델을 제안하는 컴퓨터 과학자들의 수가 증가하고 있는 실정이다 [3]. 이러한 모델의 주요 아이디어는 정상인 자가(self)와 비정상인 비자가(non-self)를 구별하는 것으로 본 논문에서는 네트워크 침입 탐지를 중심으로 하며 네트워크를 자가(self)로써 감시하는 행동을 정상으로 비자가(non-self)를 비정상으로 본다. sweeps, co-ordinated공격, 인터넷 worm과 같은 많은 정교한 네트워크 침입들은 네트워크 트래픽 패턴의 이상을 감시함으로써 침입을 탐지할 수 있다 [8]. 대부분 네트워크 기반의 IDS들은 네트워크 패킷이나 이러한 네트워크 침입들의 중요한 이상 신호를 감시한다 [5],[10].그러므로, 인공 면역 모델은 비정상적인 네트워크 행동이나 다양한 침입을 탐지하기 위해 네트워크 정상적 상태를 구별할 수 있도록 설계된다.

새롭게 제안된 인공 면역 시스템의 전체적인 구조는 그림1에서 보는 바와 같이 정상적 네트워크상태 구분 작업의 하나의 영역으로 발전되었다. 네트워크 침입 탐지를 위한 인공면역모델은 주IDS

와 보조IDS로 구성되어진다. 인간 신체 중 골수(bone marrow)와 흉선(thymus)에서는 항체(antibody)라고 불려지는 다양한 탐지 세포가 지속적으로 생산되며 살아있는 세포를 감시하기 위해 항체는 보조 임파선(secondary lymph)으로 분산되어진다. 분산된 항체들은 모든 살아있는 세포들을 감시하게 되며 특히 보조 임파선에 침입을 당한 항원(antigen)이라고 불려지는 비정상적인 세포를 탐지한다. 인공 면역모델에서 보조 IDS는 골수나 흉선으로 볼 수 있으며 이곳에서 많은 탐지기를 생산한다. 그림1의 구조는 단일 네트워크 도메인인을 위한 것으로 입력된 모든 네트워크 패킷들은 우선적으로 라우터에서 감시되어진 후에 단일 네트워크 도메인으로 옮겨진다. 개개의 탐지기들은 이러한 네트워크 트래픽 패킷에 비정상적 패턴을 기술한다. 그것은 유일(unique)한 것이며 각각의 로컬 호스트들에게 전송되어진다. 본 논문에서는 보조 임파선 노드를 로컬 호스트로 탐지기를 항체로 그리고 네트워크 침입은 항원으로 여기고 있다. 로컬 호스트인 보조IDS에서 탐지기는 로컬 호스트의 비정상적 네트워크 트래픽 패턴을 감시하기 위한 백그라운드 처리를 수행하며 주IDS와 각각의 보조IDS는 각각 다른 IDS에게 정보를 전송하기 위한 통신장치를 가지고 있다.



<그림 1> 인공 면역 모델의 물리적 구조



<그림 2> 인공 면역 모델의 개념적 구조

본 논문에서는 효과적인 네트워크 기반의 IDS를 설계하기 위하여 세 가지 중요 목표 분산화, 자가조직화, 경량화로 정하였다. 이러한 목표들은 인간 면역 시스템중의 몇몇 정교한 절차로 가능하며 이러한 절차에 초점을 맞추게 된다. 본 절에서 제안하고 있는 인공면역체계에 대해 이러한 절차들은 세 가지 진화적인 단계를 가진다. 세 가지 단계는 유전자 라이브러리 진화(gene library evolution), 부정적 선택(negative selection)과 유전자 복제(clonal selection)이다. 현재 존재하는 컴퓨터 면역 모델들은 그들이 인지한 목적에 따라 단일 단계의 사용측면을 집중시키는데 비해 본 논문에서는 새로운 인공 면역 모델의 내부에 이러한 세 가지의 중요한 진화론적 단계를 조합하였다. [3],[4],[5]. 인공 면역 모델의 전체적 개념 구조는 그림2와 같다. 그림2에서 단계1은 유전자 라이브러리 진화를 가리키며, 단계2는 부정적 선택을 단계3은 유전자 복제를 보여주고 있다. 각각의 단계들에 대한 기능과 위의 세 가지 단계 에서의 공동 처리에 대한 방법은 다음에 나올 주IDS와 보조IDS를 설명한다.

3.1 주IDS (Primary IDS)

주IDS는 처음의 두 진화과정: 유전자 라이브러리 진화와 부정적 선택을 수행한다. 유전자 라이브러리 진화 단계에서는 효과적인 탐지를 위해 일반적 지식을 얻는 것에 그 목표로 둔다. 부정적 선택 단계에서 이것은 능동적으로 경쟁하지 않고 로컬 호스트에 분산시키기 위한 단일 탐지기 집단의 수를 전송하는 다양한 탐지기의 수를 생산하는 것을 목표로 한다._이러한 작업들을 달성하기 위하여, 다음의 구성 요소들(그림2에서 보여진)을 포함한다. 첫 번째 단계인 유전자 라이브러리에서는 진화과정을 통한 생산이나 유지가 이루어진다. 인공면역모델의 유전자 라이브러리는 탐지기 가능성이 보이는 유전자들을 저장하며 다양한 유전적 절차를 통해 새로운 탐지기들을 만들어낸다. 가능성이 있는 유전자란 변칙적인 네트워크 트래픽 패턴을 기술하기 위한 행동들을 지니고 있는 것 들이다. 이들은 네트워크 프로토콜의 세부적인 절차나 그들의 보안 결점을 이해한 후에 선택된다 [8]. 초기의 유전자들은 이미 알려져 있는 침입을 흉내내었을 때 발견되는 이러한 부분의 값으로써 지정된다. 이들은 구체적으로 짧은 시간이나 한번의 연결시간동안 일반적인 네트워크 서비스들에 대한 패킷, 바이트, 특정 에러, 등등의 집합으로 기술될 수 도 있다 [5],[8]. 만약 새로운 탐지기가 처음의 유전자로부터 생성되고 로컬 호스트에 전달된다면, 변칙적인 네트워크 트래픽 활동을 탐지하게

된다. 이러한 탐지기를 포함하는 유전자는 유전자 라이브러리에 더해지게 될 것이다. 그러나, 만약 유전자가 벌써 유전자 라이브러리에 저장되어 있다면, 이러한 유전자의 값은 증가되어진다. 또는 이러한 과정이 지속될 경우 유전자 라이브러리의 크기가 계속 증가하게 될 것이다. 그러나, 만약 제안된 크기를 유지하는 유전자 라이브러리라면, 크기는 항상 고정적인 길이로 증가하게 되며 낮은 조절 값을 갖는 유전자는 유전자 라이브러리로부터 제거되고 만다. 이러한 절차는 인공 면역 모델이 유전자 라이브러리 진화를 수행할 수 있도록 하며 이러한 과정에서 인공면역 모델은 일반적으로 이전의 탐지 여부에 관계없이 존재하는 침입 부주의에 대한 지식을 학습할 수 있도록 함으로써 그것을 스스로 조직화한다. 게다가, 스스로 조직화하는 특성은 IDS가 경량화되는 발판이 된다. 이것은 이전에 탐지되었던 침입에 대한 모든 정보를 IDS가 포함하지 않기 때문이다. 대신에, 오랫동안 살아남은 유전자의 수는 그리 많지 않으며 그 수가 제한적이다.

두 번째 단계에서, 유전자 표현과정은 선택된 유전자들을 재정리를 위한 다양한 pre-detector를 만들어낸다. 유전자들의 돌연변이를 결정하는 gene-joining 포인트의 선택은 유전자 라이브러리로부터 임의로 선택된다. 이 장치는 유전자들의 조합으로 얻어진 pre-detector의 많은 숫자를 생산한다. 이러한 과정은 인공면역모델에서 경량화된 탐지기의 적은 수만으로도 다수의 침입을 탐지하는 것을 가능하게 한다. 자동화된 프로파일링 구성요소는 능동적 프로파일에서 아직 가공되지 않은 네트워크 패킷의 방대한 용량을 줄여준다. 능동적 네트워크 트래픽 프로파일의 부분들은 생산된 pre-detector를 식별하며 이러한 부분들의 구체적인 값들은 관찰된 네트워크 활동들이 정상(능동적 프로파일)인지 혹은 변칙적인지를 결정하게 된다. 그러나, 약간의 pre-detector는 그들이 유전자 표현처리에서 새롭게 생산된 돌연변이를 가지기 때문에 잘못된 탐지기가 될 수도 있다. 이러한 잘못된 pre-detector는 자동화된 프로파일러(profiler)를 이용하여 능동적으로 생산된 네트워크 프로파일을 pre-detector와 비교하는 부정적 선택 과정을 거쳐 제거된다. 만약 pre-detector의 부분 값이 능동 네트워크 트래픽 프로파일의 부분 값과 비교된다면 우리는 이러한 새로운 pre-detector를 부당하게 변칙으로 생산된 비정상적 탐지기로 생각할 수 있으며 이러한 탐지기들은 긴급히 제거된다 [4]. 이러한 과정은 자가(self)에 대한 어떠한 전체적인 정보 없이 자가(self)를 표현함으로써 잘못된 pre-detector를 제거하는 것으로 그것은 자가조직화(self-organization) 특성을 보인다.

결국, 부정적 선택과정에서 살아남은 탐지기는 분별력 있는 탐지기가 된다. 각각의 탐지기 집단이 각 개인적 로컬 호스트에 전송되기 전에 성숙한 탐지기들을 구성하는 유전자들은 유전자 라이브러리에 새롭게 등록된다. 탐지기의 집단과 능동적 네트워크 트래픽 프로파일은 로컬 호스트들에게 탐지기를 전송하기 위하여 각각의 네트워크 연결을 기반으로 성숙한 탐지기를 선택한다. 이러한 선택은 개개의 탐지기 집단의 유일성을 보장한다. 이러한 유일한 탐지기 집단은 로컬 호스트의 레벨과 독립적으로 네트워크 침입을 탐지하며 인공면역모델이 분산화 되는 것을 가능하게 한다. 선택된 탐지기 집단과 능동적 네트워크 트래픽 프로파일은 두 개의 경로를 통하여 전송되어지며 탐지기는 그들이 대응되는 보조 IDS들에게 분산된다.

3.2 보조 IDS

보조IDS는 마지막 진화 단계인 유전자 복제를 수행한다. 유전자 복제 단계의 주요 업무는 탐지기 집단의 제한된 수를 가지고 다양한 침입을 탐지하는 것이다. 동등한 탐지기를 복제하는 것은 기억탐지기를 생산하거나 주IDS에서 유전자 라이브러리 진화를 조절함으로써 수행된다. 이러한 작업은 몇몇의 구성요소들: 자가 네트워크 프로파일, 유일한 탐지기 집단, 네트워크 트래픽의 이상 탐지, 탐지기의 유전자 복제, 기억 탐지기와 통신장치의 작용으로 달성된다. 네트워크 트래픽 이상 탐지를 수행하기 위해 유일한 탐지기 집단의 탐지기와 주IDS로부터 전송된 능동적 네트워크 프로파일이 비교된다. 우선, 탐지기의 영역 값과 능동적 프로파일로 측정된 값 사이의 길이를 비교한다. 이러한 길이가 미리 정해진 임계치(threshold)값을 넘어섰을 때 이것은 통신장치에게 통보된다. 이러한 정확한 바인딩은 인공 면역 모델이 경량화되는 것을 돕는다. 이것은 만약 그들의 배합길이가 임계치를 넘었을 때 하나의 탐지기는 다른 침입의 집단을 바인딩 할 수 있기 때문이다 [6].

이상을 탐지한 후에 보조 IDS는 유전자 복제를 수행한다. 새로운 탐지기가 비정상적인 네트워크 트래픽 활동을 감지했을 때, 이러한 탐지기는 보조 IDS와 세포 자신의 기억 탐지기로써 남아있다. 복제된 탐지기는 다른 호스트에 전달될 수 있으며 그들은 오용탐지기로 작동한다. 이들은 이전에 탐지된 동일 침입에 대하여 미래에 정확한 탐지를 가능하게 한다. 게다가, 탐지기의 유전자는 주IDS에서 만약 그들이 유전자 라이브러리에 존재하지 않거나 이러한 유전자들의 적합한 값이 다른 상태로 증가된 것이라면 유전자 라이브러리에 추가되거나 갱신될 것이다. 이러한 것은 주 IDS의 유전자 라이브러리 진화를 조절하게 된다. 로컬 호스트에서 탐지기의 이상 탐지는 계속되며 각각의 로컬 호스트들이 더 많은 메모리 탐지기를 가지고 있어야 하기 때문에 각각의 로컬 호스트에 전송되어지는 탐지기의 수는 감소 된다. 이러한 과정은 모델이 자가 조직화와 경량화되는 것을 가능하게 하며 특정한 침입에 대해 미리 정의된 정보를 가지고 있는 대신 현재 존재하는 침입을 탐지함으로써 가장 바른 탐지조절을 능동적으로 편성한다. 게다가, 진화된 유전자 라이브러리와

기억 세포는 다양한 새 탐지기를 만들어내기 위한 수고를 덜어주며 모델의 경량화를 돕는다.

네트워크 침입에 대한 마지막 결정 과정은 몇몇 로컬 호스트들로부터 수집된 결정에 따라 진행된다. 인공 면역 모델은 에이전트 통신 장치를 사용한다. 의심이 가는 활동이 어떠한 보조 IDS의 이상 탐지 과정에서 탐지되었을 때 통신장치에게 신호를 보내게 되며 통신장치는 위험 수준을 증가시키고 다른 호스트들이나 주IDS에게 신호를 보낸다. 신호를 받은 다른 통신장치들도 위험 수준을 증가시킨다. 만약 의심스러운 활동이 짧은 시간 내에 몇몇 호스트에서 발견되면 각각의 호스트들과 주IDS의 위험수준이 긴급히 증가된다. 이러한 위험 수준 값의 일정한 임계치를 넘어섰을 때, 통신장치는 사용자 인터페이스를 통하여 관리자에게 네트워크 침입의 돌파를 통보할 수 있다.

3.3 인공 면역 모델의 요약

위에서 언급되어진 인공면역모델은 주IDS와 보조IDS들로 구성된다. 이것은 세 가지 진화 단계로 결합된다. 유전자 라이브러리 진화는 진화의 첫 번째 단계를 흉내내는 것으로 일반적으로 존재하는 항원들에 대한 지식을 학습한다. 이러한 과정은 모델로 하여금 경량화와 자가 조직화를 가능하게 한다. 유전자 표현과 부정적 선택은 진화의 두 번째 단계의 형태이며 자가 조직화 방법을 이용하여 잘못된 pre-detector를 제거함으로써 여러 가지의 pre-detector와 선택된 분별력 있는 탐지기 집단을 생성한다. 유일한 탐지기 집단을 보조 IDS에 전송하는 것 또한 이 단계에서 발생되어지며 모델을 분산화 시킨다. 유전자 복제는 진화의 세 번째 단계로 정확에 가까운 바인딩을 이용하여 탐지기의 제한된 수로 다양한 침입을 탐지하며 기억 탐지기를 생성한다. 이것은 보편성과 효율성을 이용해 모델의 경량화를 최대화하는 것이다. 게다가, 이러한 과정은 주IDS에서의 유전자 라이브러리 진화를 조절하게 된다. 이러한 세 가지 진화 과정들은 효과적인 IDS의 요구사항을 만족시키기 위한 디자인의 세 가지 목표: 분산화, 자가 조직화 그리고 경량화를 가능하게 하기 위해 네트워크에서 상호 협동적으로 작동하게 된다.

4. 인공 면역 모델의 검토

본 논문에서 제안된 새로운 인공 면역 모델 접근법들에 대한 이점을 입증하기 위해 우리는 네트워크 기반의 이상 탐지 요구사항들에 대한 고려와 함께 이를 현재 분석중이다. 또한 본 논문에서는 적합한 네트워크 기반의 IDS에 대한 일곱 가지 요구사항을 명세 하였으며 본 절에서 제안된 인공 면역 모델은 이러한 일곱 가지 요구사항을 고려하여 평가되어졌다.

본 절에서 제안된 인공 면역 모델은 로컬 침입을 탐지하기 위해 로컬 보조 IDS에서 유일한 탐지기 집단을 이용하여 분산화 되었으며 네트워크 침입 탐지에 대한 보조 IDS의 사이에 통신기능을 사용하였다. 이러한 분산된 특징은 모델로 하여금 robust, configurable, extendible와 scalable을 제공한다. 첫 번째로, 인공 면역은 robust하다. 어떠한 로컬 호스트에 위치하는 탐지기 집단의 실패가 다른 전체의 인공면역체계를 해치지 못한다. 설지어 아주 사소한 이상 일지라도 정확한 탐지가 가능하기 때문이다. 각각의 탐지 집단은 주 IDS의 실패에도 불구하고 네트워크 침입을 탐지하기 위하여 남아있을 수 있다. 이러한 것은 각각의 로컬 호스트들이 법칙 주IDS의 실패 전에 전송된 탐지 집단을 가지고 있기 때문이다. 이에 비해서 만약 침입자가 로컬 호스트를 통하여 탐지기가 어떻게 비정상적 행위를 탐지하는지에 대한 정보를 얻게 된다면 침입자는 얻은 정보를 이용하여 자신의 행동을 숨기려 할 것이다. 그러나, 각각의 탐지기 집단들에 대한 유일성은 이러한 시도를 어렵게 만들 수 있다. 두 번째로, 인공 면역 모델은 configurable하다. 탐지기는 주IDS에서 생성되어 지며 그들의 유용함은 각각의 보조IDS에서 세포복제를 함으로써 로컬 레벨에서 입증되었다. 게다가, 이러한 로컬 레벨의 세포 복제는 주IDS에서 유전자 라이브러리 진화를 조절한다. 다시 말해서, 생성된 탐지기는 다양한 침입을 탐지하기 위하여 공진화하며 이러한 공진화는 각각의 로컬 레벨에서의 자가 프로파일이나 자가 조직화에 의해 수행된다. 세 번째는, 인공 면역모델은 extendible을 가진다. 새로운 로컬 호스트가 네트워크에 추가되었을 때, 그것은 간단히 새로운 로컬 호스트에 대한 다른 탐지기 집단을 생성하는 것을 필요로 하며 다른 호스트 없이도 통신장치나 세포 복제 과정, 이상 탐지 과정, 자동화 프로파일 생성기로 구성되는 보조 IDS를 설치하기만 하면 된다. 이러한 구성요소들은 전체적으로 다른 보조 IDS의 구성요소들과 독립적이며 인공면역모델이 확장하는데 용이하다. 네 번째는, 인공면역모델은 scalable을 가진다. 처음의 단락 부분에서 인공면역 모델은 많은 탐지기들의 생성을 필요로 하였다. 그러나, 더욱더 많은 이상을 탐지하는 것으로써 각각의 로컬 호스트들은 더욱 더 많은 기억 탐지기를 가지게 되며 실제적으로는 매우 적은 새로운 탐지기의 전송을 요구하게 될 것이다. 그럼에도 불구하고 이러한 것은 실질적으로 짧은 시간 안에 다양한 침입의 수에 대한 발생을 요구한다. 그러므로, 전체적인 인공면역장치는 짧은 시간동안의 침입 횟수를 표현함으로써 실험되어야 할 것이다. 그리고 이러한 것은 인공 면역 모델에 의해 실제의 침입감시를 시작하기 전에 처음 학습 과정에서 이뤄진다.

인공 면역모델은 유전자 라이브러리 진화, 부정적 선택 그리고 유전자 복제를 수행함으로써 자가 조직화가 가능하게 된다. 자가 조직화의 이러한 특성은 모델로 하여금 전체 분석에 적응할 수 있는 능력과 유능한 면을 둘 다 가질 수 있도록 한다. 첫

번째로, 부정적 선택 과정은 탐지기가 어떠한 순간에도 스스로 정보를 역동적으로 고려할 수 있도록 한다. 유전자 복제와 유전자 라이브러리 진화는 가장 최근에 발생된 침입에 빠르게 적응할 수 있는 다양한 종류의 탐지기를 산출해낸다. 그러므로, 새롭게 산출된 탐지기들은 현재 존재하는 침입에 대하여 항상 역동적으로 학습을 한다. 더욱이, 새로운 침입이 탐지되었을 때, 새로운 이상 패턴은 주 IDS의 유전자 라이브러리에 등록되며 보조IDS에는 기억 탐지기로 남게된다. 그러므로, 인공 면역모델은 여전히 가장 우수한 적응성을 가지게 된다. 두 번째로, 전체 분석은 주IDS와 보조IDS 사이의 통신을 통하여 이루어지며 이러한 통신 장치는 간단하고 자율적이며 전체 통신 관리자를 필요로 하지 않는다.

결국, 인공 면역 모델은 정확한 바인딩(binding)과 기억 세포들을 이용하여 다양한 침입을 탐지함으로써 경량화될 수 있으며 이는 유전자 라이브러리 진화와 유전자 표현을 수행할 수 있도록 한다. 이러한 경량화의 특징은 좋은 효율성을 제공한다는 것이다. 첫 번째로, 정확한 바인딩은 하나의 탐지기가 다른 침입의 종류들을 탐지할 수 있도록 한다. 따라서, 본 모델은 이미 알려지거나 예상될 수 있는 침입의 수보다 더 적은 수의 탐지기 생성을 필요로 한다. 두 번째는, 위에서 언급했듯이 유전자 복제는 로컬 호스트에 기억 탐지기를 생성한다. 기억 탐지기의 수가 증가함에 따라 결과적으로 처리 시간의 절약을 위해서 새로운 탐지기들 수의 감소를 요구한다. 더 중요한 것은 지속적인 침입의 탐지와 같이 유전자 라이브러리는 유용한 유전자들을 수집한다는 것이다. 유전자 라이브러리 진화를 통하여 이러한 유전자들은 변칙을 분류함으로써 탐지기의 유용성을 입증시킨다. 이후에 탐지기들은 어떠한 시간에 프로파일의 유용한 특성만을 이용하게 되는데, 이러한 것은 각각의 로컬 호스트가 프로파일링 하는 동안 특별한 처리를 하는 요구를 제거한다. 이것은 분명히 상호 보완적 접근법에 비해 로컬 호스트를 감시하는데 발생하는 과부하를 줄인다. 시스템에서의 효율성의 최종적 단계는 유전자 표현과정으로 이러한 과정은 인공면역모델이 유전자 라이브러리에서 유전자의 적은 수를 가지고 방대한 양의 탐지기를 산출할 수 있도록 한다.

5. 결론

본 논문에서는 현존하는 네트워크 기반의 IDS를 조사하였다. 그것은 세 가지 다른 접근법: 단일 구조, 계층구조 그리고 상호 협동적인 접근법으로 분류되며 각각의 접근법에 대한 문제점을 확인하였다. 이러한 문제를 해결하기 위하여 본 논문에서는 새로운 인공면역 모델을 제안하였다. 이 모델은 세 가지 진화론적 단계: 유전자 라이브러리 진화, 부정적 선택과 유전자 복제가 하나의 단일 방법론에 합해 있도록 하였다. 이러한 방법론은 IDS의 효과적인 설계를 위한 세 가지 목표: 분산화, 자가 조직화 그리고 경량화를 만족시키기 위하여 네트워크에서 동등하게 작용된다. 이러한 통합된 진화론적 접근법에 대한 특성을 분석해보면 네트워크 기반의 IDS에 대한 요구사항을 만족시키기 위해 제안된 인공 면역 모델은 기존에 존재하던 접근법들과 유사하지 않다는 것을 알 수 있다. 결과적으로, 이러한 모델에 기반을 둔 알고리즘은 미래의 IDS에 대해 밝은 전망을 보이고 있다.

인공면역모델을 이용하는 네트워크 기반의 IDS는 본 논문에서 이러한 접근법의 타당성을 입증하는 역할을 하였다. 현재의 작업은 자가적으로 초기의 프로파일을 생성하는 것과 실제 네트워크 환경에서 수집된 정상과 비정상적인 TCP/IP 패킷을 가지고 탐지기를 개발하는데 그 초점을 두고 있다.

7. 참고문헌

[1] Balasubramaniyan, J. S. et al., 1998, "An Architecture for Intrusion Detection using Autonomous Agents", Department of Computer Sciences, Purdue University, Available at http://www.cs.purdue.edu/coast/coast-library.html

[2] Carlberg, K.(SAIC), Dec.1998, personal communication.

[3] Dasgupta, D.; Attoch-Okine, N., 1997, Immunity-Based Systems: A Survey , *Proceeding of the IEEE International Conference on Systems, Man and Cybernetics*, Orlando.

[4] Forrest, S.; Hofmeyr, S.; Somayaji, A., 1997, "Computer Immunology", *Communications of the ACM*, vol.40, No.10, pp.88-96. Available at http://www.cs.unm.edu/~forrest/papers.html

[5] Mykerjee, B., et al, 1994, "Network Intrusion Detection", *IEEE Network*, Vol.8, No.3, pp.26-41.

[6] Somayaji, A.,; Hofmeyr, S.; Forrest, S., 1997, " Principles of a computer immune system", *Proceeding of New Security Paradigms Workshop, Langdale, Cumbria*, pp.75-82.

[7] Porras, P. A.; Neumann, P. G., 1997, "EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances", *Proceeding of 20th National Information System Security Conference*. Available at http://www.csl.sri.com/emerald/downloads.html

[8] Porras, P. A.; Valdes, A., 1998, Live Traffic Analysis of TCP/IP Gateways",*Proceeding of ISOC Symposium of Network and Distributed System security*. Available at http://www2.csl.sri.com/emerald/downloads.html

[9] Staniford-Chen, S., et al., 1996, "GrIDS – A Graph-Based Intrusion Detection System for Large Networks", *Proceeding of the 19th National Information Systems Security Conference*. http://seclab.cs.ucdavis.edu/papers.htm

[10] Tizard, I. R., 1995, *Immunology: Introduction*, 4th Ed,

Saunders College Publishing.
[11] White, G. B.; Pooch, U; Fisch, E. A, 1996, "Cooperating Security Managers: A Peer-Based Intrusion Detection System , *IEEE Network*, Vol.10, No.1, pp.20-23.