인간 면역 체계를 이용한 네트워크 탐지기술 연구 [1)]

김정원[*] · Peter Brently[**] · 정길호[***] · 최종욱[****]

A Study on Network detection technique using Human Immune System

Jungwon Kim[*], Peter Brently, [**], Gilho Jung[***], Jonguk Choi[****]

요 약

This paper reviews and assesses the analogy between the human immune system and network intrusion detection systems. The promising results from a growing number of proposed computer immune models for intrusion detection motivate this work. The paper begins by briefly introducing existing intrusion detection systems (IDS's). A set of general requirements for network-based IDS's and the design goals to satisfy these requirements are identified by a careful examination of the literature. An overview of the human immune system is presented and its salient features that can contribute to the design of competent network-based IDS's are analysed. The analysis shows that the coordinated actions of several sophisticated mechanisms of the human immune system satisfy all the identified design goals. Consequently, the paper concludes that the design of a novel network-based IDS based on the human immune system is promising for future network-based IDS's.

Key words: 컴퓨터 면역 체계(Computer Immune System), 인간 면역 체계(Human Immune System), 네트워크 침입 탐지(Network Intrusion Detection)

1. 서 론

침입 탐지 시스템(Intrusion Detection System)은 컴퓨터 시스템 침입을 탐지하기 위한 자동화 시스템이다. 이러한 침입탐지시스템의 주된 목표는 시스템의 외·내부에서 컴퓨터 시스템에 대한 인정되지 않은 사용이나 오용 등을 탐지하는 것이다. 방화벽이나 암호화 같은 시스템보호 연구와 유사하게 IDS에 대한 중요성이 강조되고 있으며 다양한 접근법이 제시되거나 개발되고 있다. 또한 새로운 접근법을 통해서 몇몇의 컴퓨터 과학자들은 침입이나 컴퓨터 바이러스 탐지에 대한 간단한 컴퓨터 면역 모델들을 제안하고 있다 [4][5][6][9]. 이러한 모델들로부터 얻어진 결과들은 컴퓨터 과학자들로 하여금 인간 면역 체계를 충분히 이해시키기 위한 동기를 부여하고 있다.

본 논문에서는 새로운 네트워크 침입탐지 모델에 대해 성공적으로 적용하기 위해 인간 면역 체계의 주요 특징들을 살펴보고 이를 인공적으로 개발하는데 그 목표를 두고 있다. 인간 면역 체계 중에서도 침입한 병원체들을 탐지할 수 있는 몇 가지의 우수한 특성들이 조심스럽게 연구되어지고 있으며 이러한 특성들을 네트워크 침입 탐지에 적용하기 위한 가능성이나 이익들이 조사되거나 평가되고 있다.

본 논문은 다음과 같은 내용으로 구성되어진다. 우선, 다음 절에서는 기존 침입탐지시스템을 간단히 설명하고, 3절에서는 네트워크 기반의 침입탐지시스템에 대한 요구사항들의 개요를 설명한다. 4절에서는 3절에서 제시한 요구사항들을 만족시키기 위한 세 가지의 네트워크 기반 IDS의 설계 목표를 소개한다. 그리고 5절에서는 인간 면역 체계에 대해서 소개하고 6절에서는 인간 면역 체계의

1) 본 연구는 과학기술부 국제공동연구 (I-03-002)의 지원에 의해 수행되었슴.

[*] Universe college of London
[**] Universe college of London
[***] 상명대학교 정보통신학부
[****] 상명대학교 정보통신학부

중요한 특성들을 분석하고 네트워크 기반 침입탐지 시스템들의 설계 목표들을 비교한다. 본 논문의 마지막 부분에서는 실질적인 네트워크 환경에서의 인공면역 모델 개발을 위한 Prototype을 보이고 이러한 작업과 미래에 수행돼야 할 작업들로부터 도출된 결론을 제시한다.

2. 침입탐지시스템

호스트 레벨에서 수행되었던 기존의 침입탐지 시스템들이 최근에는 네트워크를 기반으로 하는 경향을 보이고 있다 [7]. 호스트 기반의 침입탐지 시스템은 호스트의 운영체제가 만들어내는 감사증적(audit trail)을 이용하여 단일 호스트 기계만을 감시하며 네트워크 기반 침입탐지시스템은 다중 호스트들이나 네트워크 트래픽을 세밀하게 검사함으로써 네트워크 상의 특정 호스트 집단을 감시한다.

호스트 기반 또는 네트워크 기반의 침입탐지 시스템은 비정상행위탐지(anomaly detection)와 오용탐지(misuse detection)의 두 기능을 탑재하고 있다 [7]. 비정상행위 탐지 접근법은 사용자, 시스템, 시스템 자원, 네트워크 트래픽과 서비스에 대한 정상적인 프로파일을 작성한다. 그런 후에 프로파일에서 조사된 정상적인 행동 패턴으로부터 중요한 이상행위(misuse signature)를 확인함으로써 침입을 탐지한다. 오용 탐지 접근법은 이미 알려진 시스템 취약성과 보안 정책에 기반을 두고 의심스러운 오용 신호를 정의 내리는 접근 방법이다. 이러한 접근법은 오용 신호가 표시되거나 감사증적에 없는 것들에 대하여 면밀한 조사를 한다. 이 두 가지 기술은 서로 다른 강점과 약점을 가지고 있으며 완벽한 침입탐지시스템을 위해서는 상호간의 협력이 필요하다 [7].

본 논문에서는 인간 면역 체계와 네트워크 기반 침입탐지 시스템간의 분석을 중점적으로 소개하고자 한다. Somayaji etal[9]은 컴퓨터 면역 시스템에 대한 더욱 일반적인 원리를 소개하였으며 다양한 가능성을 제시하였다. 반대로 본 논문은 적합한 네트워크 기반 침입탐지시스템의 설계에 그 집중을 두었으며 인간 면역 체계의 두드러진 특성들을 분석하였다.

3. 네트워크 기반 침입탐지시스템의 필요

네트워크 기반 침입탐지시스템을 설계에 필요한 기능들을 이해하기 위해 앞에서 소개된 인간 면역 체계의 특성들을 살펴볼 필요가 있다. 인간 면역 체계의 7가지의 중요한 기능들은 다음과 같다.

Robustness: 다중 탐지 기능을 가지는 것으로 IDS들이 공격을 받거나 어떠한 시스템 결함이 발생했을 때 이에 대해 충분히 강인한 다중 탐지 기능을 가져야만 한다[1][4]. IDS의 치명적인 약점은 침입자의 행동에 의한 시스템 실패나 파괴에 약하다는 것이다. 만약 침입자가 이미 IDS의 존재를 알고 있다면 그것을 파괴할 수 있으며 그렇게 되면 IDS를 발전시키기 위한 노력은 아무런 효과가 없게 된다..

Configurability: 각각의 호스트들과 각각의 네트워크 구성 요소들의 지역적 요구사항을 스스로 간편하게 형성할 수 있어야 한다[1][9]. 네트워크 환경에서 개개의 호스트들은 서로 이질적이다. 그러므로 이들은 다른 각각의 고유한 보안 사항을 가지게 된다. 게다가 호스트들에게 라우터(router), 필터(filter), DNS, 방화벽 또는 다양한 네트워크 서비스 같은 네트워크 구성 요소들은 다양한 보안 요구사항을 갖고 있을 수도 있다. 따라서 이에 대한 탄력적인 구조를 지녀야 한다.

Extrendibility: 새롭게 추가되는 호스트들에 대해 IDS의 감시 범위를 확장하기 쉬어야 한다[1][9]. 만약 새로운 호스트가 기존의 네트워크 환경에 추가되었을 때 특히 이러한 새로운 호스트가 다른 운영체제를 바탕으로 한다면 이는 다른 형식의 감사자료(audit data)를 가지게 된다. 그것은 기존의 IDS를 기반으로 하고 있기 때문에 이를 동일한 방법으로 감시하는 것은 간단하지 않다.

Scalability: 분산된 호스트들로부터 방대한 양의 감사자료를 모으거나 분석하기 위한 신뢰성 있는 검사능력을 갖추어야만 한다[1]. 단일 IDS의 경우 감사증적 수집 과정이 분산화 되어있으며 자료의 분석만이 중앙에 집중된다[9]. 그러나, 데이터 손실 없이 모든 감사증적을 분석하기 위하여 하나의 IDS에 이러한 자료를 미리 전송하는데 많은 어려움이 있다. 심지어 만약 모든 감사 자료를 정확하게 헤아린다면 그것은 급속하게 네트워크 성능을 감소시킨다.

Adaptability: 역동적으로 변화하는 네트워크침입을 탐지하기 위해서는 동적으로 적응되어야만 한다 [1][9]. 컴퓨터 시스템 환경은 고정적이지 않으며 사용자, 공급자 그리고 시스템 관리자들은 항상 시스템 환경을 변화시키기 때문에, 네트워크와 침입의 정상 행위들은 이러한 환경이 변함에 따라 지속적으로 변화한다.

Global Analysis: 네트워크 침입을 탐지하기 위해서는 방대한량의 증거를 수집하고 각각의 이벤트들 사이의 관계를 식별하는 다양한 호스트에서 생성된 사건들을 종합적으로 감시해야만 한다[1][7]. 많은 네트워크 침입은 종종 네트워크상에서 여러 지점을 거쳐서 이루어지기 때문에 단일 호스트에서는 단순히 정상적인 문제점으로 인식되기도 한다. 그러나 만약 다중 호스트에 의해서 다중 지점을 종합적으로 감시할 경우, 이러한 여러 지점을 거친 침입은 명백하게 하나의 단일 공격 시도로 확인된다.

Efficiency: 감시되고 있는 호스트 시스템과 네트워크에게 최소의 과부하(overhead)를 주기 위해 단순화와 경량화(lightweight)되어야만 한다[1][5][9]. 단일 침입탐지시스템은 네트워크를 감시하기 위해 자료 수집, 자료 처리와 의사결정 등을 하는데 이것은 시스템으로 하여금 많은 과부하를 주게 될 것이며 CPU와 I/O에 과중한 작업을 부과하게 된다. 결과적으로 시스템과 네트워크의 성능이 저하된다.

지금까지 매우 다양한 접근방법이 제안되고 개발되었음에도 불구하고, 여전히 어떤 네트워크 기반 모형도 위의 요구사항들을 완벽하게 만족시키지 못하고 있다[1],[7].

4. 네트워크 기반 침입탐지시스템의 설계 목표

앞서 분류된 요구사항들을 효율적으로 만족시키기 위하여 다음의 기능들을 침입탐지시스템 설계 목표로 유도할 수 있다.

4.1 분산화(distribution)

첫 번째 설계 목표는 분산화 하는 것이다. 분산된 네트워크 기반의 침입탐지시스템은 기존의 주 IDS의 역할을 다른 구성요소들에게 위임한다. 독립적인 침입 탐지 프로세스들은 오직 전체시스템의 작은 일부분만을 감시하는 것으로 분산된 IDS들은 각각 다른 구성요소들과 동시적이거나 협력적으로 수행된다. 만약 네트워크 기반의 침입탐지시스템이 분산화 되어 있다면 그것은 다음의 요구사항을 만족시킬 것이다.

Robustness: 분산된 네트워크 기반의 IDS에서 어떠한 로컬 침입탐지공정의 실패가 전체 IDS의 장애가 되지 않으며 이러한 실패는 전체 탐지 정확성에 있어서 최소의 저하만을 가져온다.

Configurability: 단일 침입탐지공정은 다른 호스트들의 다양한 요구사항에 대한 고려 없이 특별한 호스트를 위주로 로컬 요구사항을 맞추는 것이 가능하게 된다.

Extendibility: 다른 운영체제에서 실행되고 있는 새로운 호스트도 네트워크에 추가될 수 있으며 이러한 호스트를 이용하여 새로운 침입 탐지 공정을 탐지 목록에 쉽게 갱신할 수 있다. 이는 침입 탐지 공정이 독립적이므로 기존에 존재하는 공정들에게 새로운 침입 탐지 공정이 더해지더라도 기존의 공정을 수정할 필요가 없도록 한다.

Scalability: 감시되고 있는 로컬 호스트에서 감사자료 수집과 분석이 수행되므로 다량의 감사자료들은 로컬 호스트들에게 분산된다. 그러므로, 분산된 IDS들은 하나의 중앙 서버를 기반으로 하는 IDS보다 더욱 우수한 scaling능력을 가진다.

4.2 자가조직화(self-organization)

두 번째 목표는 자가조직화 하는 것이다. 중앙의 조절장치가 없이도 미리 정의된 정보를 가지며 능동적으로 조직화하는 네트워크 기반의 IDS는 자동적으로 기존에 알려지지 않은 침입 신호를 학습한다. 이러한 것은 다양한 보안 요구사항이나 다른 침입 탐지 프로세스 같은 변화하는 네트워크 환경에서도 상호작용을 통해 목적을 달성하게 된다. 만약 네트워크 기반의 침입탐지시스템이 자가조직화를 수행한다면 이것은 다음과 같은 요구사항들을 만족시킬 것이다.

Adaptability: 이것은 네트워크 환경 변화에 따른 침입 신호에 대하여 손수 갱신해야 할 필요가 없기 때문에 높은 적응력을 보여준다.

Global analysis: 전체 침입탐지시스템은 간편한 전체적 분석을 수행한다. 이러한 것은 탐지기가 다양한 침입탐지 공정을 이용한 상호작용을 통해 자가조직화를 하기 때문이다.

4.3 경량화(Lightweight)

세 번째 설계 목표는 경량화이다. 경량화된 네트워크 기반 침입탐지시스템은 CPU나 I/O에 무리한 과부하(overhead)를 주지 않는다. 만약 네트워크 기반 IDS가 경량화된다면 다음과 같은 요구사항을 만족시킬 것이다.

Efficiency: IDS의 각 구성요소들에게 최소한의 작업만을 부과함으로써 주 작업은 로컬 호스트에서 수행되므로 네트워크는 감시로 인한 영향을 받지 않는다.

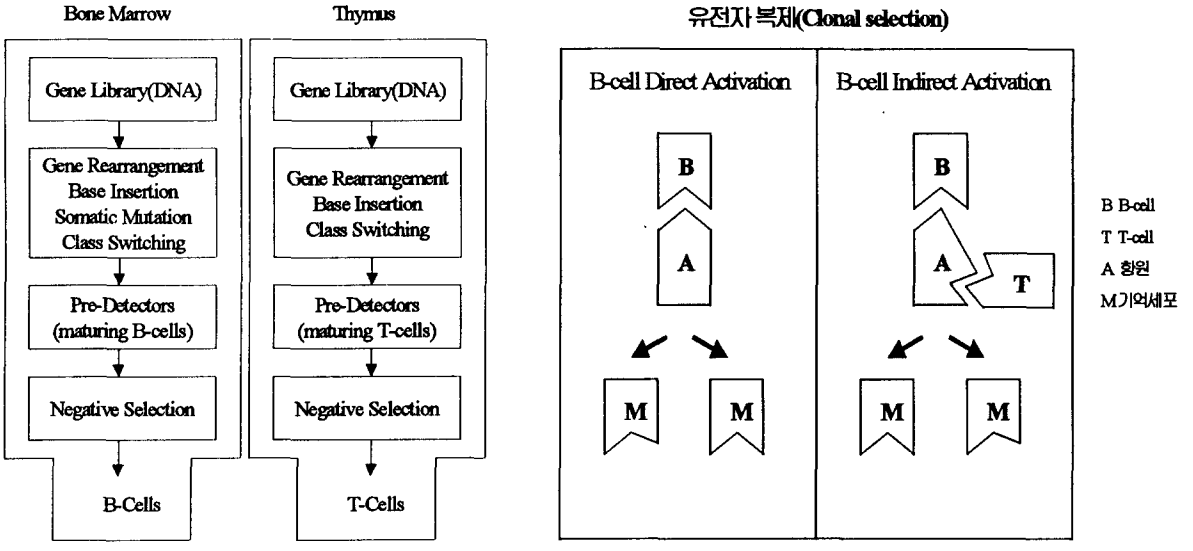
5. 인간 면역 체계 개요

앞에서 우리는 인간 면역 체계의 특징이 네트워크 기반의 침입탐지시스템의 효율적 설계에 유용하다는 것을 증명하였다. 또한 그것은 인간 면역 체계의 중요한 장치들에 대한 조사의 필요성을 강조하기도 한다 [8][10]. 이 부분에서 우리는 개략적인 것에 대해 언급하려고 한다. 전체 인간 면역 체계는 한가지 특정한 인체 기관의 기능보다는 선천적이거나 후천적으로 얻어진 다양한 종류의 세포들의 상호작용으로 이뤄진다. 서로 다른 거대한 수의 세포들에게 임파구(lymphopcytes, 백혈구들)는 중요한 역할을 담당한다. 이같은 중요한 장치들은

인체의 세포들인 자가세포와 위험한 외부 세포인 비자가세포를 구별하는 역할을 한다. 각각의 임파구는 항체(antibody)와 같은 이미 알려져 있는 유해한 외래 세포들에게 조직적인 집단 반응을 보이는 것으로 특성화된다. 임파구는 수용체(receptor)라는 특정한 자기 구역을 가지고 있으며 항체의 결정소(determinant)를 구성하기 위해 상호 보완적으로 활동한다. 특정한 항원은 자신의 에피토프(epitope)를 임파구 항체의 수용체를 바인딩 함으로써 인지하기도 한다.

임파구는 크게 B-cell과 T-cell 두 가지로 분류되는데, B-cell은 항원 분비 세포이고 T-cell은 항원을 죽이기도 하며 B-cell의 성장을 억제하거나 도와주는 역할을 하는 세포이다. B-cell과 T-cell 모두 유일한 유전자 구조를 가지고 있다. B-cell과 T-cell은 몇몇 DNA(유전자 라이브러리)의 체인으로 표현되며 각각의 체인은 변동 영역과 고정 영역을 가지고 있다. 변동 영역의 유전자들은 하나의 유전자로부터 다른 것들로 크게 변화되며 이러한 것은 항원들로 하여금 명확한 영역을 결정짓게 한다. 고정 영역에서의 유전자들은 변화하지 않으며 B-cell 항체의 수용체가 항원의 에피토프를 바인딩 할 때 다양한 생물학적 효과가 나타난다. B-cell과 T-cell은 각각의 골수(bone marrow)나 흉선(thymus)에서 성장한다. 골수와 흉선 부분에서 몇몇의 유전자 라이브러리들(gene libraries)은 B-cell과 T-cell의 영역에 반응하는데 이는 B-cell과 T-cell 수용체를 생산 시킬 수 있는 지원 유전자(candidate gene)에게 반응하기 위해서다. 특별한 수용체들은 유전자 라이브러리와 그것에 참가하는 것들로부터 유전자 조각을 임의로 선택해 생성된다.

이러한 것은 유전자 재배열, 다른 결합 부분에 대한 선택, 신체적 돌연변이, 클래스 스위칭 그리고 이외의 다른 것들을 포함하고 있다 [10].



<그림 1> B-cell과 T-cell의 성장(좌측). 유전자 복제(우측)

골수와 흉선을 떠나기 전에 성장한 B-cell과 T-cell은 마지막 단계인 부정적선택(negative selection) 과정을 통과한다. B-cell과 T-cell 진화과정에서 전체적으로 새로운 세포 수용체들은 다양한 유전적 조작자에 의해서 생성된다. 그러므로, 그것은 자가 세포 에피토프들을 바인딩 하기 위해 임으로 생산된 수용체들에 대한 가능성을 배제시킨다. 이러한 것을 보호하기 위하여 성장한 B-cell과 T-cell이 골수와 임파구를 순환하는 자가세포를 바인딩 하려고 할 때 그들은 신체에 방출되지 않고 그대로 제거된다. 그림 1(좌측)에서는 골수와 임파구에서 B-cell과 T-cell이 성장하는 것을 보여준다.

성장한 B-cell과 T-cell은 골수와 임파구로부터 방출되어 부정적 선택 과정을 통과한다. B-cell과 T-cell 모두 활동이나 번식을 위해 지속적으로 혈액 또는 도중에 마주치게 된 항원을 거쳐 신체를 순환하게 되며 B-cell의 항체는 직접적이거나 간접적으로 활성화된 항원들을 바인딩 함으로써 위험스러운 항원을 인지한다. B-cell 항체의 수용체가 임계치(threshold)의 상위에서 강한 유연(affinity)을 가지고 항원의 에피토프를 바인딩할 때 그것들은 직접적인 활성화가 된다. 다른 한편으로, B-cell은 T-cell의 도움을 필요로 하며 Major-Histocompatibility Complex (MHC) 분자의 활성화를 필요로 한다. MHC 분자들은 B-cell의 활성화를 돕기 위한 두 가지 기능을 가지고 있다. 첫 번째는, MHC 분자는 임시로 세포 내에 숨어있는(세포의 표면에서 보이지 않는) 항원들

의 조각들을 바인딩 한다. 두 번째는, MHC 분자는 B-cell의 표면에 바인딩 한 조각들을 전송한다. 약한 유연을 지닌 B-cell 항체의 수용체가 항원의 에피토프를 바인딩 할 때, MHC 분자는 세포 내에 숨어있는 다소의 항원들을 찾기 위하여 노력한다. MHC 분자가 그러한 항원들을 찾았을 때 B-cell의 표면에 이를 전송시킨다. T-cell의 수용체는 B-cell 표면에서 MHC분자를 인지하도록 유전적으로 구조화되어 있다. T-cell이 강력한 유연을 가지고 MHC 분자를 바인딩 할 때 그것은 MHC 분자의 식별과 성장을 활성화하기 위하여 특별한 화학적 신호를 전송한다. B-cell과 T-cell의 중요한 차이 한가지는 오직 B-cell만이 골수에서 성장할 때 그것의 변화를 증가시키기 위하여 매우 높은 돌연변이 율을 가진다는 것이다. 이와 같이, B-cell은 매우 다양하고 새로운 T-cell을 가지게 된다. 게다가 골수가 분산되어지는 동안 임파구는 중앙에 위치하게 된다. 자가 세포의 대부분은 임파구를 통과하게 되며 이러한 것은 임파구에서의 부정적 선택이 골수를 통과한 것보다 더 신뢰적이라는 것을 알 수 있다. 그러므로, 약한 유연을 가진 B-cell 활동의 최종적인 결정은 T-cell에 의해서 만들어진다.

T-cell의 보조가 있건 없건 간에 B-cell은 활성화 되어지며 이러한 활성화는 일시적으로 유전자 복제를 지향한다. 활성화된 B-cell은 부모 B-cell 혹은 변이 된 항원-바인딩 특성과 같은 것을 가지는 유전자들의 집단으로 나눠진다. 다른 한편으로 만약 어떠한 항원이 일정 시간 내에 B-cell을 활성화시킬 수 없다면 그들은 신속하게 제거된다. 그러므로, 기존에 존재하는 항원을 기반으로 한 오직 적응력을 지닌 B-cell 항체만이 살아 남는 것이다. 항원은 지속적인 변화를 하기 때문에 탐지 효율에 있어 유전자 복제를 통해 B-cell 항체를 진화하는 방법으로 효율성을 유지시킨다. 항원이 B-cell을 활성화시켰을 때 그들은 미래에 동일한 항원의 재발생에 대처하기 위해 기억세포를 생산한다. 이러한 기억세포를 이용하면 기존에 확인이 되었던 항원들은 더 빠르게(두 번째 반응으로 알려져) 탐지가 가능하다. 그림1(우측)에서는 유전자 복제에 의한 기억세포들의 생성을 보여준다.

반대로, 항항체들(anti-antibodies)인 유전자형 항체들은 항체의 수용체들을 활성화시킬 수 있다. 면역 시스템은 항원과 항항체로 하여금 항체에게 바인딩 할 수 있도록 하며, 승리한 항항체가 항체와 항원사이에서 발생하는 바인딩을 진압할 수 있도록 한다. 항원에 대한 유전적 항체의 진압은 면역 반응의 적당한 수준을 조절하는데 도움을 준다. 면역학자인 Jern은 유전적 항체의 역할을 이해하는데 기본을 두고 있는 면역 네트워크 이론을 제안하였다 [2],[3]. 그는 면역 시스템이 임파구의 기능적인 네트워크이며 어떠한 순간에 이 네트워크는 항체와 항원의 내부 상호작용의 동적인 상태를 가진다고 보았다. 항원에 대한 식별과 유전적 항체에 의한 진압의 끊임없는 반복은 거대한 규모의 네트워크를 형성할 수 있다. 결국 이러한 네트워크는 통제와 감시를 통한 안정적인 상태에 도달했을 때 그것이 전체 면역 시스템을 결정하게 된다.

6. 네트워크 기반 IDS 대한 인간 면역 체계의 특성

인간 면역 체계의 복잡한 능력에 대한 조심스러운 분석은 위와 같이 요약될 수 있다. 이러한 능력은 네트워크 기반 침입탐지에 대한 몇몇의 중요한 특성을 확인시켜준다. 위의 조사에서, 상세한 특성들은 네트워크 기반 침입탐지시스템의 3가지 설계 목표(분산화, 자가조직화, 경량화) 각각을 만족시킴으로써 상호 작용될 수 있다는 것을 알 수 있다.

6.1 분산화(Distribution)

인간 면역 체계는 분산화 되어 있다. 다음의 장치들은 인간 면역 체계로 하여금 실제적인 분산 환경에서의 항원 탐지를 가능하게 한다.

Immune Network : 인간 면역 체계는 서로 다른 다양한 종류의 세포들이 상호작용을 수행함으로써 이뤄진다. 중앙 조정자(co-ordinator)를 두는 대신에 인간 면역 체계는 유전적 항체들을 이용한 항체 진압과 활동사이의 안정적인 상태를 유지함으로써 면역 반응의 적당한 수준을 유지한다 [2],[3].

Unique Antibody Sets : 인간 면역 체계는 항원들을 탐지하기 위한 항체들의 다양한 수를 형성한다. 이러한 진화 장치들은 유전자 라이브러리의 선천적 선택(natural selection)과 유전자복제를 통하여 항체들의 다양한 수를 유지시킨다. 그러므로, 각각의 항체 집합은 유일하거나 독립적인 특성을 가진다. 이러한 특성은 어떠한 중앙의 조정자를 필요로 하지 않으며 그들은 인간 면역 체계가 지역적인 항체 수준에서 항원들을 탐지하도록 한다 [9].

6.2 자가조직화(self-organizing)

전체 면역 반응은 다음의 세 가지 진화단계로 구성된다. 유전자 라이브러리(gene library) 진화는 효율적인 항체를 생산하며, 부정적 선택(negative selection)은 부적절한 항체를 죽인다. 마지막으로 유전자 복제(clonal selection)는 제대로 수행되고 있는 항체를 복제한다. 이러한 세 가지 단계들은 중앙 조직 혹은 미리 정의된 정보를 이용한 직접적인 수행보다 더 자가조직화 된다.

Gene Library Evolution : 항체는 오직 항원에 있는 보완적인 특성으로써 항원을 인지한다. 그러므로, 항원의 특성에 대한 다소의 지식들은 유능한 항체를 생산하기 위해 요구되어진다. 인간 면역 체계는 진

화 시간이 지남으로써 이러한 지식들을 학습하게 되며 우리들에게 효율적이거나 지식이 풍부한 DNA를 제공한다. 이러한 진화적인 자가 조직 과정 때문에 유전자 라이브러리는 흔히 판별된 항원들을 어떻게 탐지하느냐에 대한 정보를 기록하는 방법으로 수행된다 [10].

Negative selection : 두 번째 과정으로, 이 과정에서 부적당하거나 일시적으로 존재하는 모든 항체들이 제거된다. 면역 체계에서 중요시 여겨지는 전암은 자가 세포들을 만족시키기 위해 공격하지 않게 된다. 자가세포들에 대한 어떠한 전체적인 정보를 가지는 대신에 이러한 감제적인 목표 달성은 골수와 임파구에서 자가 세포를 보여줌으로써 수행되며 이 세포를 공격하는 항체들은 제거된다 [4][8].

Clonal Selection : 세 번째 과정으로, 이러한 과정은 현재 잘 수행되고 있는 항체들을 복제한다. 항체들은 수명이 다한 후에 급히 제거되므로 현재 존재하는 항원에 적응을 가장 잘 수행하고 있는 항체만이 살아 남게 된다. 이와 유사하게, 특정한 항원에 대해 미리 정의된 정보를 가지고 있는 대신 그것은 자신이 가장 잘 맞는 항체를 현재 존재하는 항원과 접목시킴으로써 자가조직화를 수행한다 [8],[10].

6.3 경량화

인간 면역 체계는 경량화 되어 있다. 다음에 나오는 장치들은 경량화를 가능하게 하며 다음의 세 가지 아이디어에 중점을 두고 있다. i) 많은 수의 항원들이 적은 수의 항체들에게 어떻게 탐지될 것인가. ii) 이미 알려져 있는 항원 정보가 효율적으로 어떻게 재사용 되나. iii) 다양한 항체들이 유전자의 제한된 수만으로 어떻게 생산될 수 있나. 대략적인 바인딩(approximate binding)과 기억세포(memory cell) 그리고 유전자 표현(gene expression)은 이러한 질문들에 대한 정확한 대답을 제공한다.

Approximate Binding : 면역 반응은 항체와 항원사이의 바인딩 유연이 큰 폭으로 상승하였을 때 활성화된다. 다른 말로, 하나의 항체는 그들의 유연이 상승할 수 있을 만큼의 어떠한 항원 집단을 탐지할 수 있다. 이러한 근접 바인딩은 면역 체계의 보편성을 증가시키는 역할을 한다[4].

Memory Cells : 메모리 세포는 기존에 탐지되었던 항원 에피토프들의 유전적 정보를 저장하며 그들이 미래에 전과 동일한 항원을 만났을 경우 신속하고 효율적으로 반응한다[9][10]. 기억 세포는 보통의 항체들보다 더 긴 생명주기를 가지고 있기 때문에 그들은 동일한 항체를 다시 만들어야 되는 요구 없이도 면역성을 그대로 유지한다.

Gene expression : 면역 체계는 항원들의 광범위한 범위에 대해 효율적 탐지를 보장함으로써 항체 변화를 유지한다. 항체의 성장 과정에서 유전자 라이브러리로에서 다양한 항체들을 형성하기 위하여 유전자 표현과 같은 몇몇의 유전적 장치들을 합체하고 있다. 이러한 장치들의 주 아이디어는 새로운 항체들의 많은 수가 유전자 라이브러리에서 유전자 조각의 새로운 조합만으로 생산될 수 있게 하기 위한 것이다. [8][10].

요약해보면, 이러한 분석은 인간 면역 체계가 면역 네트워크와 고유한 항체 집단들을 통해 분산화되는 것을 보여주고 있다. 그것은 유전자 라이브러리의 진화, 부정적 선택, 유전자 복제의 3가지 진화론 과정들이기 때문에 자가조직화(self-organization)가 가능하다. 또한 대략적인 바인딩의 보편성과 유전자 표현, 그리고 기억 세포의 효율성을 지니고 있기 때문에 경량화(lightweight)가 가능한 것이다.

그러므로, 인간 면역 체계는 분산화, 자가 조직화 그리고 경량화되어 있으며 네트워크 기반의 침입탐지시스템의 설계 목표를 명백하게 이행시킨다. 면역체계에서 중요한 위의 장치들은 인간 면역 체계가 IDS의 3가지 설계 목표를 만족시킴으로써 훌륭한 방법으로 적용될 수 있으며 미래 연구 장치들에 대한 동기를 부여하게 된다. 본 연구에서 네트워크 기반 침입탐지에 인간 면역 체계를 접목시킴으로써 다른 전체 접근법들에게 중요한 이익을 제공한 것으로 볼 수 있다.

7. 결론

본 논문에서는 네트워크 기반의 침입탐지시스템에 대하여 연구하였으며 학계에서 평가되고 있는 침입탐지의 일반적인 요구사항들을 소개하였다. 이러한 요구사항들에 기본을 두고 3가지 중요한 설계 목표들이 확인되어졌으며 이러한 목표를 만족시키기 위한 인간 면역 체계의 여러 가지 현저한 특성들을 살펴보았다. 특히 위에서 강조한 장치들은 네트워크 기반의 침입탐지시스템으로 하여금 요구사항을 만족시키는 탐지 시스템의 구축이 가능하도록 하였다. 따라서, 인간 면역 체계를 이용한 새로운 네트워크 기반의 침입탐지시스템 설계는 미래의 네트워크 기반 침입탐지시스템에 대한 가망성을 제시한다.

현재의 작업은 실제 네트워크 상에서의 감시가 가능한 더 자세한 인공 면역 모델의 창조를 포함하고 있다. 특히, 이 작업은 6절에서 실제 네트워크 환경 하에서의 네트워크 기반 침입탐지 시스템의 설계 목표를 달성하기 위하여 인간 면역 체계의 몇몇 핵심 장치들을 설계하는데 그 초점을 두고 있다.

8. 참고문헌

[1] Balasubramaniyan, J. S. et al., 1997, "Software Agents for Intrusion Detection", Department of Computer

Sciences, Purdue University, available at http://www.cs.purdue.edu/coast/coast-library.html

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

[3] Farmer, J. D.; Packard, N. H.; Perelson, A. S., 1986, The Immune System, Adaptation and Machine Learning , *Physica* 22D, pp.182-204.

[4] Forrest, S.; Hofmeyr, S; Somayaji, A, 1997, "Computer Immunology", *Communications of the ACM*, Vol.40, No.10, pp.88-96.

[5] Forrest, S. et al., 1996, "A Sense of Self for Unix processes", *Proceedings of 1996 IEEE Symposium on Computer Security and Privacy*, Los Alamos, CA, pp.120-128.

[6] Kephart, J. O., 1994, "A Biologically Inspired Immune System for Computers", *Artificial Life IV, Proceeding of the Fourth International Workshop on the Synthesis and Simulation of Living Systems*, pp.130-139.

[7] Mykerjee, B.; Heberlein, L. T.; Levitt, K. N., 1994, "Network Intrusion Detection", *IEEE Network*, Vol.8, No.3, pp.26-41.

[8] Paul, W. E., 1993, The Immune System: An Introduction , in *Fundamental Immunology* 3rd Ed., W. E. Paul (Ed), Raven Press Ltd.

[9] Somayaji, A.; Hofmeyr, S.; Forrest, S., 1997, " Principles of a Computer Immune System", *Proceeding of New Security Paradigms Workshop, Langdale, Cumbria*, pp.75-82.

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