한국 퍼지 및 지능시스템학회 논문지 2000, Vol. 10, No. 2 (2000)122~128

생체 면역시스템 기반의 새로운 보안 항체 계층 모델

An Immunity-based Security Antibody Layer Model

구자범 · 이동욱 · 박세현 · 심귀보

Ja Beom Gu, Dong-Wook Lee, Se Hyun Park and Kwee-Bo Sim

중앙대학교 전자전기공학부

요 약

호스트는 인터넷을 통한 혁신적인 공격(innovative antigen)을 신속하게 감지하고 제거할 수 있는 새로운 자율적, 지능적 보안 시스템의 구현을 필요로 한다. 그러나, 단독의 호스트가 이러한 공격에 대처할 수 있는 능력은 시스템 및 네트워크 자원의 제한으로 그 한계를 들어내고 있다. 본 논문에서는 생체면역체계를 기반으로 급속히 다양해지는 인터넷 공격에 대해 효율적으로 신속히 대처를 할 수 있는 Antibody Layer(다변화된 자율 면역 시스템)를 제안한다. Antibody Layer는 다양한 등급의 보안 서비스(Security QoS Class)를 제공해 주며, 혁신적인 공격에 대해 호스트 단독으로 대처할 뿐만 아니라, 광대한 호스트 연합을 구성하여 공동으로 대처하므로 보다 질 높은 보안 서비스를 실시간으로 제공할 수 있다.

ABSTRACT

With the rising innovative antigens(such as intruders and viruses) through Internet, new secure schemes are expected to perceptively detect and put them down. However, the current hosts over Internet could not properly analyze Internet antigens due to limitations of their system and network resources. In this paper, we introduce an Antibody Layer that mediates proper security services based on the biological mechanism to rapidly disclose and remove innovative antigens. The proposed Antibody Layer also provides three classes to make agreed-on security parameters set up easily with respect to real-time security QoS for one host as well as host alliances.

1. 서 론

최근 인터넷의 급속한 보급은 다양한 사용자로 하여금 시간과 공간의 제약을 벗어나 시스템(PC, 서버, PDA)의 접속을 용이하게 한다. 특히 악의적 사용자들은 인터넷의 유동성을 기반으로 특정 시스템에 침입하여 정보를 유출하거나 파괴하며, 바이러스를 수동적, 능동적으로 유포한다. 이러한 악의적 공격의 시도와 성공은 최근 급격히 증가하고 있으며, 전자상거래의 활성화 및 유무선 인터넷의 보급과 함께 더욱 문제를 유발시킬 것으로 예상된다.

이러한 공격에 대해서, 각각 인터넷 기반의 시스템은 독립적으로 방어기술을 수립하거나, 몇몇 상용화된 소프트웨어에 의존하여 대처하고 있는 것이 현재의 추세이다. 그러나, 이미 알려지거나 노출 가능한 방어기술은 일반화된 인터넷 침입 등에는 효율적으로 대처할 수 있으나, 좀더 지능적 혹은 진화된 침입에 사용하기엔 매우 위험하다. 더욱이 인터넷상에서 새로운 백신을 받아서 급속히 변화하는 인터넷 침입 추이에 대처하는 것은, 인터넷을 통한 중요한 통신 기술 추세가 실시간 응용 프로그램이고 바이러스나 해커의 본질이 마코브 체인에 기반 한다는 점을 감안하였을 때, 효율적인 해결책이 될 수 없다. 설령 인터넷상에서 시스템간의 방어기술을 공유한다고 하더라도, 새로운 침입의 생성 비율 및 기존 침입 정보 양의 방대함으로 인해, 시스템 객체가 실시간 또는 최단의 서비스 시간에서 인터넷 공격을 차단하는 것은 가능하지 않다.

본 논문에서는 이러한 문제점을 생체 면역시스템에서 각 세포의 역할 및 관계를 모델링하여 이를 실제 시스템에 적용하여 해결하고자 한다. 생체 면역시스템은 B-세포(B-cell 또는 B-림프구)와 T-세포(T-cell 또는 T-림프구)로 구성되어 있다. 각각의 면역세포는 항원을 직·간접으로 퇴치하는 기능을 할 뿐 아니라, 시시각각으로 변화하는 환경 속에서 자신을 존속시키는 중요한 기능을 하고 있다. 또한 각종 림프구 세포는 상호간에 정보교환을 통하여 적합한 항체를 증식시키기 위한 고도의 정보처리 시스템, 즉 면역네트워크를 구현하고 있다[1,2]. 본 논문의 새로운 보안 시스템은 이러한 자율 면역계를 현재 및 차세대 인터넷에 적합

하게 모델링하여, 인터넷 항원(공격)에 대해 능동적으로 대처할 수 있게 하였으며, 적절한 보안 서비스 등급의 지정으로 그 효율성을 높이는데 목적이 있다.

2절에서는 Antibody Layer의 구조와 기능에 대해 기술하고, 3절과 4절에서는 Anti-Antigen Procedure (AAP) Mechanism과 면역네트워크 그룹에 대해 각각 설명한 후, 5절에서 Security QoS Class를 정의하고, 6절에서 결론을 맺는다.

2. Antibody Layer

인터넷상의 시스템, 즉 호스트에 대한 항원(침입자와 바이러스)의 공격은 날로 다양해지고 있다. 또한 항원의 급속한 전파 속도 때문에 단독의 호스트는 이에 대한 적절한 대응을 하지 못하고 있다. 이러한 문제점을 해결하기 위해, 본 논문에서 호스트가 혁신적이고 다양하게 진화된 공격을 보다 효율적으로 감지하고 제거할 수 있는 Antibody Layer(다변화된 자율면역 시스템)를 제안한다(그림 1).

Antibody Layer는 Basic Antibody(B-세포) Layer, Evolved Antibody(T-세포) Layer, Threat Information Bank, Anti-Antigen Procedure(AAP) Mech-anism, 그리고 그룹관리모듈로 구성된다. 특히 Basic Antibody Layer와 Evolved Antibody Layer는 생체 면역시스템(Biological Immune System)을 모델로 하여, B-세포가 공격을 감지, 제거하고 T-세포는 B-세포를 도와 병렬분산처리 알고리즘을 이용한 면역네트워크를 구성하여 공격에 신속하게 대처하도록 한다. 이는 생체 면역 시스템의 B-세포의 항체 생성작용과 림프구들 간의 상호정보교환 작용을 모델링한 것이다. Antibody Layer는 TCP/IP와 응용프로그램의 중간에 위치하며 상·하위 계층과의 연결은 Layer Service Provider가 담당하고 있다. AAP는 Antibody Layer의 각 부분을 연결(3절)하고, 그룹관리모듈(4절)은 암호화된 데이터의 전송을 담당한다.

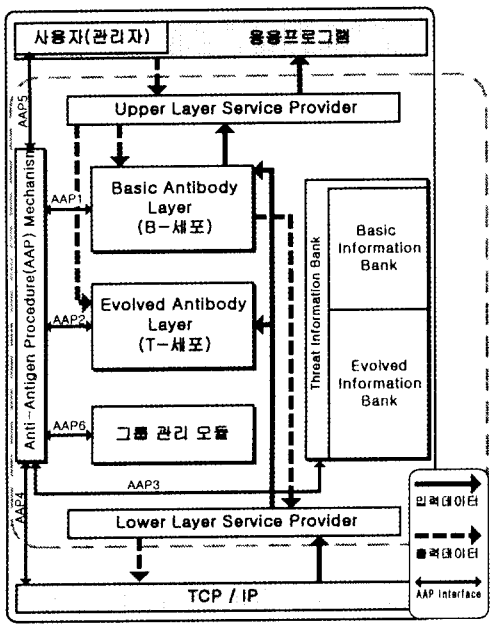


그림 1. Antibody Layer의 구조

2.1 Threat Information Bank

Threat Information Bank는 두 개의 Information Bank로 구성된다. 하나는 Basic Information Bank로 이미 알려진 인터넷 항원에 대한 정보(항체정보)들이 들어있다. Basic Antibody(B-세포) Layer는 Basic Information Bank의 내용을 기반으로 비교검색을 수행하므로 빠른 검색을 위해서 Basic Information Bank의 면역정보는 핵심적인 내용만을 담고 있어야 한다. 이 Basic Information Bank는 각 호스트의 Antibody Layer에서 공유한다. 다른 하나는 Evolved Information Bank로 각 호스트의 Antibody Layer마다 다변화된 항체 정보들이 생성·저장된다. 이것은 동일한 인터넷 항원에 대해서도 호스트마다 다른 검색결과를 만들 수 있다. Evolved Antibody(T-세포) Layer는 Basic Information Bank와 Evolved Information Bank의 내용을 기반으로 검색을 수행한다.

2.2 Basic Antibody Layer(B-세포)

Antibody Layer의 핵심은 실시간으로 효율적인 보안 서비스를 제공하여 시스템이 공격에 자발적으로 대처할 수 있는 능력을 부여하는데 있다. 이를 위하여 B-세포는 모든 데이터를 비교 검색하여, 데이터가 공격인지 아닌지를 판별한다. B-세포는 단순한 비교검색만을 수행하므로 새로운 공격에 대한 검색은 할 수 없지만, 검색 속도는 매우 빠르기 때문에 실시간으로 진행될 수 있다.

2.3 Evolved Antibody Layer(T-세포)

Evolved Antibody Layer는 Basic Infor-mation Bank와 Evolved Information Bank의 내용을 조합하여 이로부터 현재의 데이터나 사용자 작업이 새로운 형태의 공격인지를 판단하게 된다. 이러한 유추작업은 활용 가능한 모든 항원정보(이전의 공격에서 얻어진 작업형태, 중요 파일에의 변화 등)를 이용해야 하므로 Evolved Information Bank의 크기는 매우 클 수밖에

없다. 따라서 이런 유추작업이 수행될 때의 문제점은 방대한 양의 면역정보로 인해 실시간으로 감지, 대처할 수 없다는 것이다. 즉, 유추작업에 사용할 데이터가 많을수록 검색에 성공할 확률은 높아지지만 작업시간 역시 늘어나므로 효율적이라고 할 수 없다. 이것은 고성능의 시스템을 가정하더라도 문제가 될 수 있으므로, 이를 해결하기 위해서 본 논문에서는 다변화된 T-세포를 이용한 병렬분산처리 기법을 사용한다. 병렬분산처리를 이용하면 방대한 면역정보로부터의 유추작업을 여러 호스트에서 나누어 실행하므로 수행시간을 획기적으로 단축할 수 있다. 이것은 T-세포가 다변화되어 있기 때문에 가능하다.

그림 2는 T-세포에서 유추작업을 수행해 처방을 생성하는 과정을 나타낸다. 그림 2-(a)에서 보듯이 T-세포 #1과 #2는 각자 자신의 Basic Information Bank와 Evolved Information Bank의 내용을 가진다. 그림 2-(b)는 T-세포 #1, #2는 각자의 면역정보를 조합하여 새로운 면역정보(처방)를 생성하고 있음을 보여준다. T-세포는 새로운 면역정보를 Basic Information Bank에 등록하고, 다른 T-세포와 정보를 그림 2-(c)와 같이 공유한다.

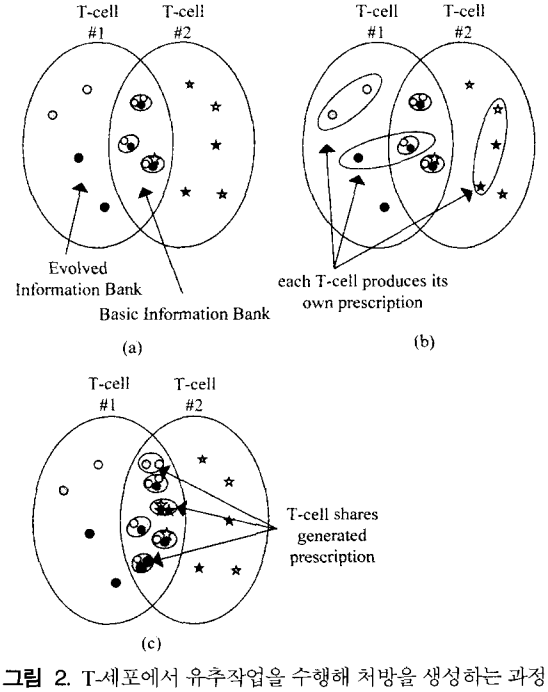


그림 2. T-세포에서 유추작업을 수행해 처방을 생성하는 과정 (a) Basic Information Bank의 내용을 두 T-세포(Antibody)가 공유 (b) 새로운 항원에 대해 각 T-세포는 나름대로 유추 (c) 유추된 결과 중 항원 제거에 핵심이 되는 내용을 공유

이와 같이 본 논문에서는 Basic Antibody Layer는 B-세포의 공격 감지기능을 담당하고 Evolved Antibody Layer는 두 가지 종류의 T-세포 즉 보조 T-세포(helper T-Cell)과 억제 T-세포(suppressor T-Cell)의 기능을 담당한다. 실제로 보조 T-세포는 B-세포의 작용을 도와주며 억제 T-세포는 항체분비의 과다함을 억제하는 역할을 한다. Evolved Antibody Layer의 기능 중에서 유추작용을 통한 Basic Information Bank의 생성은 보조 T-세포의 작용에 대응되며 여러 T-세포간의 면역네트워크를 통한 정보의 교환 및 최적의 정보 유지 메커니즘은 억제 T-세포의 작용에 대응된다.

3. Anti-Antigen Procedure (AAP) Mechanism

AAP는 Antibody Layer의 각 부분을 연결하고 있으면서 인터넷 항원에 대한 신속한 항체를 제공한다. AAP의 주된 역할은 시스템 감시, 프로세스 제어 및 감염파일 삭제, Threat Information Bank의 갱신, 다른 호스트의 Antibody와 연동 등이다(그림 3). AAP는 여러 인터페이스를 이용해 Antibody의 각 부분을 효율적으로 연결한다.

1) AAP는 AAP1, AAP2를 이용해서 B-세포, T-세포와 연결되어 검색 결과를 AAP에 통보하여 적절한 동작을 하도록 하고, AAP3을 통하여 Information Bank의 내용을 갱신한다.

2) AAP4는 다른 호스트의 AAP에 새로운 공격에 대한 공동검색을 요청하고, 그에 대한 응답을 받기 위한 인터페이스이다.

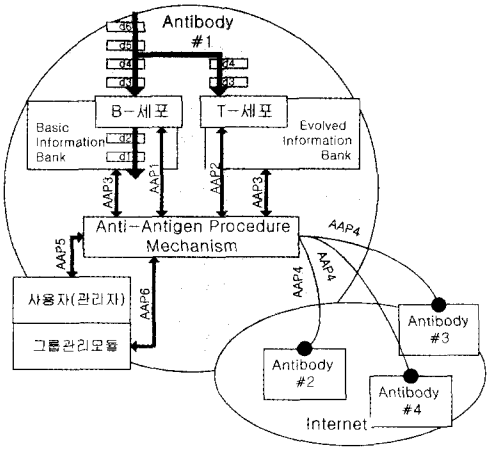


그림 3. Anti-Antigen Procedure(AAP) Mechanism의 동작

3) AAP5는 실행중인 프로세스를 제어하고, 감염된 파일을 삭제하여 공격을 제거하고, 필요한 경우 시스템으로부터 더 많은 리소스를 제공받기 위한 인터페이스이다. 또한 AAP5는 사용자 (관리자)와 연결되어 있어, 필요하면 사용자 작업을 수행할 수 있도록 한다.

4) AAP6는 그룹관리모듈과 연결되어 있다.

4. 면역네트워크 (Host Alliance)

4.1 면역네트워크 그룹의 특징

각 호스트의 Antibody Layer는 상호 정보교환을 통해 광범위한 면역 네트워크(Host Alliance)를 구성한다. 이때 B-세포의 근간이 되는 Basic Information Bank 내용을 각각의 호스트가 공유하여 이미 알려진 인터넷 항원에 대해 실시간으로 비교검색 할 수 있도록 한다. 그러나, Evolved Information Bank의 내용은 공유하지 않고 호스트 고유의 정보를 갖고 인터넷 항원에 대응하며, 만일 다른 Antibody Layer가 공동검색을 요청하면 이에 따라 검색을 수행한다. 이러한 상호간의 정보교환을 위해 면역네트워크 그룹은 효율적으로 연결되어야 하므로, 다음과 같은 특성을 기반으로 설계한다.

1) 그룹 크기: 새로운 인터넷 항원에 대해 자율적으로 대처하는 면역시스템은 그 중요도가 점점 증가할 것으로 예상되며, 이러한 면역 시스템을 이용하기 위해 면역네트워크 그룹에 가입하는 호스트 수는 매우 많을 것으로 기대된다. 또한, 핵심이 되는 Evolved Antibody Layer는 그 수가 증가할수록 효력을 발휘하므로 그룹 가입자의 수는 매우 중요하다. 그러므로 그룹의 크기는 각각의 호스트가 QoS를 고려하여 사용목적에 따라서 유동적으로 설정하는 것이 바람직하다.

2) 전송 데이터: 그룹 내에 전송되는 데이터는 Basic Information Bank의 내용을 갱신하기 위한 것과, 공동검색에 대한 요청 및 응답이다. 효율적 항원과 항체의 정보 교환을 위해 본 논문은 면역네트워크 topology를 다음 장에서 제시한다.

3) 보안성: 전송되는 데이터는 Authentication, Confidentiality, Integrity 등의 보안 서비스가 필요하다[3-5].

4.2 Topology

이러한 특징을 갖는 그룹이 효율적으로 정보를 교환하기 위한 방법으로 멀티캐스트를 이용한다. 멀티캐스팅 그룹은 보안 서비스(authentication)를 위해서 하나의 호스트(Group Controller)가 그룹멤버에게 그룹

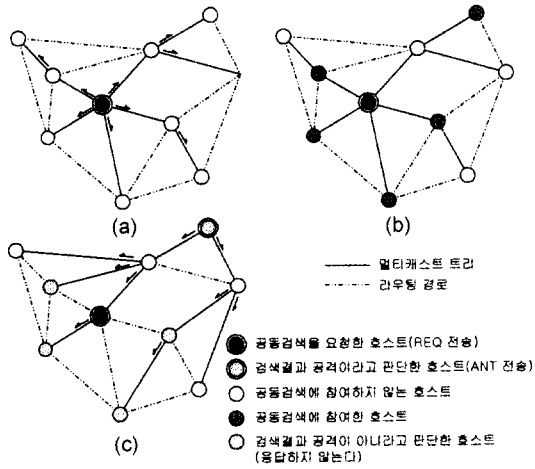


그림 4. 공동검색 요청을 따른 면역네트워크 그룹의 작용 (a) 공동검색 요청을 멀티캐스트. (b) 면역네트워크 그룹 멤버는 요청을 받아 각자 검색을 수행. (c) 공격이라고 판단한 호스트는 이를 멀티캐스트

키(Group Key)를 분배하는 중추적인 역할을 해야 한다. 각 호스트는 이 그룹 키를 이용하여 멀티캐스팅을 한다. Antibody Layer에서 이러한 역할은 그룹관리모듈이 담당한다. 즉, AAP4를 통해서 전송되는 데이터는 그룹관리모듈에서 encryption/decryption 된다.

멀티캐스팅을 이용해서 그룹내의 호스트들에게 공동검색을 요청한 경우 그 응답 속도는 호스트마다 다를 수 있는데, 그 분포는 일반적으로 Poisson 분포를 따른다. 그러나 요청에 대한 응답이 한번에 몰리는 경우(response implosion) 소규모 멀티캐스트 그룹인 경우 문제되지 않지만, 그룹크기가 커지면 문제가 될 수 있으므로 다음과 같은 응답 억제(response suppression) 알고리즘을 사용한다(그림 4).

REQ(*REQUEST*) : 공동검색 요청

ANT(*ANTIGEN*) : 인터넷 항원 경고 메시지

i. 호스트가 *REQ*전송한다(그림 4-(a)).

ii. 면역 네트워크 그룹멤버 (Alliance)는 *REQ*를 받아 각자 검색을 수행(그림 4-(b)).

iii. 자신의 검색 결과 공격이 아니라고 판단한 호스트는 메시지를 전송하지 않는다.

iv. 한 호스트로부터 ANT가 보내지면, 다른 호스트는 이를 수신하여 면역정보를 갱신하고 응답을 억제한다(그림 4-(c)).

v. 면역네트워크 그룹의 시스템 및 네트워크 자원에 따라 설정된 타이머에 의해 다음 공동검색을 위하여 ANT의 송수신을 종료한다.

vi. 전송되는 데이터는 모두 그룹 키로 암호화해서 전송한다.

vii. 공동검색 요청에 대해서 호스트는 시스템 리소스를 고려해 검색을 할지를 결정한다.

5. Security QoS Class

5.1 보안 등급 지정(security class specification)

면역 시스템은 호스트의 사용자에게 다양한 등급의 보안 서비스를 제공할 필요가 있다. Antibody Layer가 시스템 자원의 낭비를 초래하고 면역네트워크의 경우 네트워크 자원을 적절히 이용 설정하지 않을 경우 다양한 응용프로그램 및 사용자의 요구를 충족시킬 수 없으므로, 본 논문에서는 보안 QoS를 위한 세 가지 등급을 표 1과 같이 제시한다.

제 1등급은 Basic Antibody Layer에서 제공하고, 실시간으로 기존의 인터넷 항원을 감지할 수 있다. 제 2등급은 Evolved Antibody Layer에서 제공하고, Basic과 Evolved Information bank의 내용을 기반으로 알려지지 않은 새로운 항원을 감지한다. 제 3등급은 호스트 연합을 이용한 광범위한 면역네트워크를 이용하여 문제를 해결한다. 각 등급에 따른 Antibody Layer의 동작원리는 다음절에서 소개한다.

5.2 보안 등급에 따른 Antibody Layer의 동작

그림 5, 6, 7의 순서도는 보안 등급에 따른 Antibody Layer의 동작을 보여주고 있다. Antibody Layer는 모든 데이터에 대해 기본적으로 등급 1, 2의 보안 서비스를 실시간으로 제공해 준다. 이는 각 호스트가 가지는 다변화된 면역정보의 크기가 작으므로 가능하다. 등급 2의 보안 서비스를 위해 Evolved Antibody는 데이터에 대해 고유의 Information Bank (Basic, Evolved)의 내용을 가지고 자가진단을 한다. 자가진단 결과 공격인 것으로 판단이 되면, AAP는 데이터를 삭제하거나 사용자의 작업인 경우 해당 프로세스를 제어한다(그림 5). AAP는 지속적으로 시스템의 동작을 감시하여 시스템이 바이러스에 감염되거나, 공격당한 경우 사용자에 의한 치료법을 개발함과 동시에, 다른 호스트들에게 자신의 시스템 증상을 제공해 면역 네트워크에서 치료법을 개발하도록 한다(그림 6).

그림 7은 Antibody Layer가 보다 질 높은 보안

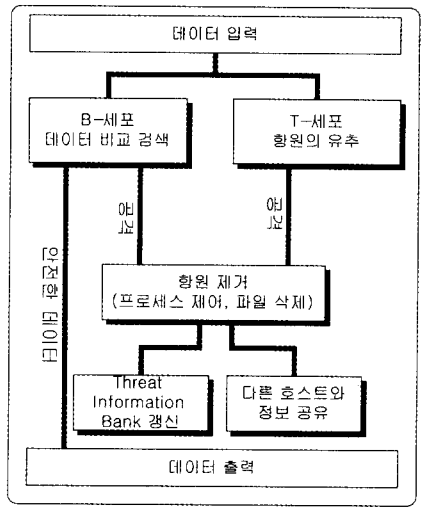


그림 5. Antibody Layer가 등급 1, 2의 보안 서비스를 제공할 때의 순서도

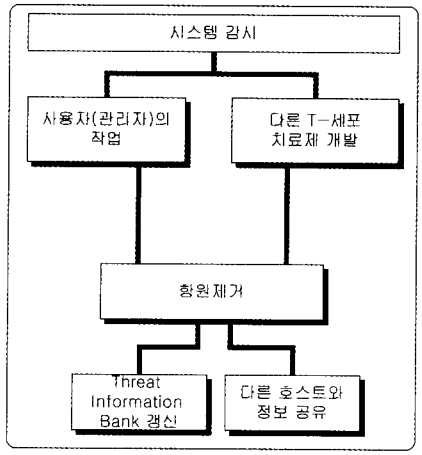


그림 6. Antibody는 지속적으로 시스템을 감시한다.

표 1. Antibody Layer가 제공해 주는 보안등급의 종류와 특징

	Class 1	Class 2	Class 3
Responding Layer	Basic Antibody	Evolved Antibody	Evolved Antibody
Scope	Local Host	Local Host	Internet
Threat Information Bank	Basic Information Bank	Basic & Evolved Information Bank	Basic & Evolved Information Bank
Detect Method	Basic Scan	Self-detection	Host Alliance

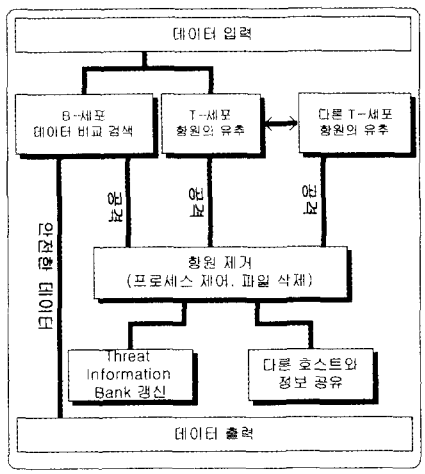


그림 7. 보다 높은 등급의 보안 서비스를 제공하기 위한 Antibody Layer의 동작

서비스를 제공하기 위해 자가진단을 수행함과 동시에 면역네트워크를 이용한 공동진단 작업을 수행함을 보여준다. 이때, 보안등급 2와 3은 데이터의 중요도와 시스템의 상황 등을 고려하여 결정하게 된다. 보안등급 3에서는 공동진단 결과 공격이라고 판단한 응답을 수신한 경우 해당 프로세스를 제어하고, 처방을 받아 치료한다.

6. 결 론

본 논문에서는 인터넷을 통한 혁신적인 공격에 대해 효율적이고 신속한 대처를 할 수 있는 시스템을 개발하기 위하여 생체 면역시스템을 모델링한 Antibody Layer(다변화된 자율 면역 시스템)를 제안하였다.

외부 항원에 대한 효과적인 대응을 위하여 B-세포는 Basic Antibody로 T-세포는 Evolved Antibody로 모델링 하였다. Basic Antibody는 Basic Information Bank를 이용하여 기본적인 항원 퇴치 기능을 담당하며 Evolved Antibody는 면역네트워크를 구성하여 다른 호스트와 정보를 교환하고 유추작용을 함으로써 Basic Information Bank의 내용 갱신 및 최적의 정보를 유지한다. 한편 각 Antibody layer는 기능에 따라 보안 등급을 지정함으로서 안전하게 각각의 기능이 수행될 수 있도록 설계하였다.

본 논문에서 제안한 Antibody Layer는 다양한 등급의 보안 서비스를 제공함은 물론이고, 광대한 호스트 연합을 구성하여 공동으로 대처하므로 호스트가 단독으로 공격을 감지하거나 이에 대처할 수 없는 경우나 보다 질 높은 보안 서비스를 요구하는 경우에도 실시간으로 서비스를 제공할 수 있는 장점을 가지고 있다.

참고문헌

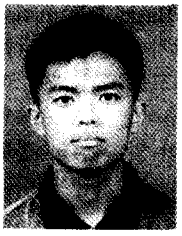
[1] I. Roitt, J. Brostoff, D. Male, Immunology, 4th edition, Mosby, 1996.

[2] D. Dasgupta, "An Overview of Artificial mmune systems and Their Applications" in Artificial Immune systems and Their Applications, Springer, pp. 3-21, 1998.

[3] PARK, S. H., GANZ, A. and GANZ, Z.: "Security protocol for IEEE 802.11 wireless local area network", Baltzer Science MONET, Vol. 3, No. 3, September, 1998, pp. 237-246.

[4] GANZ, A., PARK, S. H. and GANZ, Z.: "Robust re-authentication and key exchange protocol for IEEE 802.11 wireless LANs", IEEE MILCOM 98, October, 1998

[5] GANZ, A., PARK, S. H. and GANZ, Z.: "Security Broker for multimedia wireless LANs: design, implementation and testbed", IEEE MILCOM 99, October, 1999.



구 자 범 (Ja-Beom Gu)

2000년 : 중앙대학교 전자공학과 학사
2000년~현재 : 중앙대학교 전자공학과 석사과정
관심분야 : 인터넷 정보보호(디지털 면역시스템), 무선 LAN

이 동 욱 (Dong-Wook Lee)

1996년 : 중앙대학교 제어계측공학과 학사
1998년 : 중앙대학교 제어계측학과 석사
1998년~현재 : 중앙대학교 제어계측학과 박사과정
관심분야 : 인공생명, 인공두뇌, 인공면역계, 자율분산시스템, 가상현실 등

박 세 현 (Se-Hyun Park)

1986년 : 중앙대학교 전자공학과 학사
1988년 : 중앙대학교 전자공학과 석사
1998년 : University of Massachusetts at Amherst, 컴퓨터 공학 박사
1988년~1994년 : 한국 전자 통신 연구원
1995년~1998년 : EnRich Net
1999년~현재 : 중앙대학교 전자전기공학부 교수
관심분야 : 인터넷 정보보호(디지털 면역시스템), 무선 LAN, 가상 사설망, 셀룰러 IP, 차세대 인터넷 등

심 귀 보 (Kwee-Bo Sim)

1984년 : 중앙대학교 전자공학과 학사
1986년 : 중앙대학교 전자공학과 석사
1990년 : The University of Tokyo 전자공학과 박사
1990년 : 동경대학 생산기술연구소 연구원
1998년~현재 : 한국퍼지 및 지능시스템 학회 이사 및 논문지 편집위원
1999년~현재 : 한국 뇌학회 학술위원
1991년~현재 : 중앙재학교 전자전기공학부 교수
관심분야 : 인공생명, 진화연산, 지능로봇시스템, 뉴로-퍼지 및 소프트 컴퓨팅, 자율분산시스템, 로봇 비전, 진화하는 하드웨어, 인공면역계 등