Proceedings of KFIS 2001 Spring Conference, 2001. 5.

보안 항체계층을 위한 코오퍼레이션 프로토콜

Cooperation Protocol for Security Antibody Layer

김세진 · 구자범 · 박세현
중앙대학교 전자전기공학부

Sejin Kim, Jabeom Gu and Sehyun Park
School of Electrical and Electronic Engineering, Chung-Ang University
E-mail : goodsj@ms.cau.ac.kr

Abstract

인터넷 보안문제 해결을 위해서 침입탐지 시스템 및 바이러스 백신등이 연구되어왔고, 생체면역을 응용한 보안체계가 연구되고 있으나, 컴퓨터 자원소비와 비실시간대응의 문제점을 가지고 있다. 이에 Antibody Layer[1]는 인공면역과 Host alliance를 기반으로 하여 보안문제 해결에 효율성과 정확성을 제공하였다. 본 논문에서는 Antibody Layer의 Host alliance를 위한 Cooperation Protocol에 대하여 논하였다.

Key Words : antibody layer, host alliance, cooperation protocol, computer immune system

Ⅰ. 서론

인터넷기반의 환경에서 바이러스나 해킹 등의 보안 위협 요소(Antigen)는 점차 다양화, 지능화되고 있으며, 사용이 간단한 도구들이 제작되어 인터넷을 통해 대량 유포되면서 인터넷상의 보안은 더욱 위협을 받고 있다

이러한 공격에 대해서 각각의 인터넷 기반 시스템들은 독립적으로 방어기술을 수립하거나, 몇몇 상용화된 소프트웨어에 의존하여 대처하고 있는 것이 현재의 추세이다. 그러나 이미 알려지거나 노출 가능한 방어기술은 일반화된 인터넷 침입에는 효과적으로 대처할 수 있으나 좀 더 지능적이며 진보된 침입에는 적합하지 못하다. 또한 인터넷을 이용한 Antigen들은 러브바이러스등과 같은 예에서 볼 수 있듯이 불과 몇일만에 전세계로 확산되어 큰 피해를 줄 수 있으며, 더욱이 실시간 응용서비스가 증가하는 추세이므로 Antigen의 확산에 걸리는 시간은 더욱 짧아질 것이다. 현재의 인터넷은 정보화의 역기능에 취약한 구조로 인해 여러 가지 문제점을 가지고 있으며 폭발적으로 늘어나는 컴퓨터 네트웍 응용분야는 새로운 보안 체계를 요구하고 있다.

최근에는 기존의 침입탐지 시스템 및 바이러스 백신 등의 보안 시스템과 더불어 새로이 인공면역을 응용한 보안 체계에 대한 연구가 진행되고 있다.[3] 그러나 여전히 많은 문제점을 가지고 있으며, 본 논문의 2.1절에서 이에 대해 논하였다. 2.2절에서는 위의 시스템들에 대한 해결방안으로 제안된 Antibody[1]의 구성과 특징을 살펴보고, 2.3절에서 Antibody Layer의 핵심인 Cooperation Protocol을 구체화시키기 위해 파라미터들을 정의하고 이들의 상관관계를 살펴보았다.

Ⅱ. 본 론

2.1 기존보안체계의 문제점

기존의 침입 탐지 시스템이나 바이러스 백신 등은 공격을 detect하기 위해 공격에 해당하는 signature를 저장한다. 하지만 더 많은 공격을 detect하기 위해서는 더 많은 signature가 필요하기 때문에 데이터베이스의 크기는 비례적으로 늘어날 수밖에 없다. 이 경우 detect할 확률을 높일 수는 있으나 하나의 호스트가 이러한 수많은 정보를 모두 가지고 있기에는 저장 공간의 문제와 더불어 비용의 문제가 발생한다.[4] 또한 인공면역을 응용한 시스템의 경우, 정확도는 높일 수 있으나 생체면역을 모델링하는 과정에서 많은 계산량을 필요하게 되어 많은 자원이 소모되는 문제를 가지고 있다. 특히 이러한 문제들은 제한된 자원을 갖는 이동통신단말에는 커다란 보안취약의 요인이 될 수 있다.

기존 보안체계의 또다른 문제점으로는 인터넷을 통한 공격 방법은 급속히 증가, 진화하고 예측 불가능한 특성을 가지는 반면에 공격을 탐지하기 위한 데이터베이스의 업데이트는 수동적으로 이루어진다는 점이다. 때문에 빠른 속도로 확산되어 가는 공격에 대해 기존의 보안체계는 적절한 시간 내에 대응하는 것이 불가능하여 새로운 공격에 큰 피해를 입을 수밖에 없다.

2.2 Antibody Layer

Antibody layer[1]에서 제안된 Host alliance를 구성하는 각각의 호스트는 그림 1과 같은 보안계층의 구조를 가지며, Antibody Layer의 보안계층 각각의 구성요소는 다음과 같다.

- Basic Antibody Layer(B-세포)
- Evolved Antibody Layer(T-세포)
- Threat Information Bank
- Anti-Antigen Procedure Mechanism
- 그룹 관리 모듈

Basic Antibody Layer와 Evolved Antibody Layer는 생체 면역시스템을 모델로 하여, Basic Antibody Layer(B-세포)가 공격을 감지, 제거하고 Evolved Antibody Layer(T-세포)는 Basic Antibody Layer(B-세포)를 도와 병렬분산처리 알고리즘을 이용한 면역네트워크를 구성하여 공격에 신속하게 대처한다. 이는 생체면역 시스템의 B-세포의 항체 생성작용과 림프구들 간의 상호정보교환 작용을 모델링한 것이다. (그림 2는 이에 대한 간략한 모델을 나타낸다.) Antibody Layer는 TCP/IP와 응용프로그램의 중간에 위치하며 상·하위 계층과의 연결은 Layer Service Provider가 담당하고 있다. Anti-Antigen Procedure는 Antibody Layer의 각 부분을 연결하고, 그룹관리모듈은 암호화된 데이터의 전송을 담당한다.

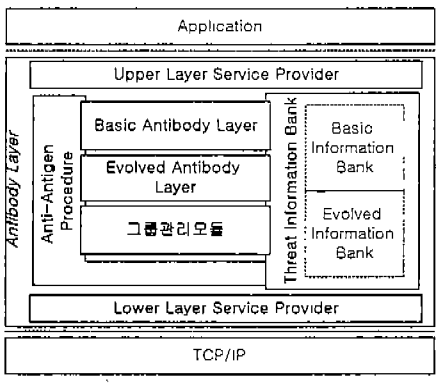

그림 1. Antibody Layer의 구조

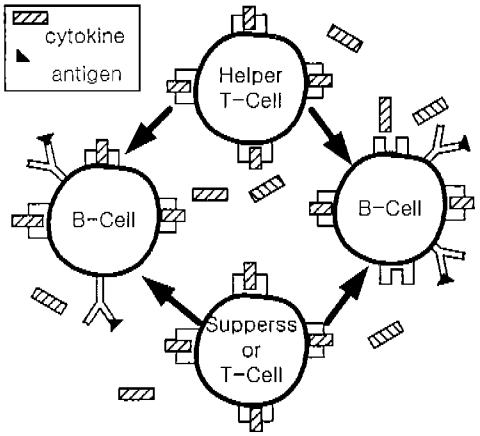

그림 2. 생체면역시스템 모델

위에서 언급한 바와 같이 Antibody Layer는 기본적으로 인공면역을 응용한 검색방법을 사용하고 효율성과 정확성을 높이기 위해 여러 호스트들이 Host alliance 그룹을 구성하여 인터넷 항원에 대해서 공동으로 대처한다. 즉, 앞에서 제시된 기존 보안체계의 문제점에 대한 해결책을 다음과 같이 제안하고 있다.

· 데이터베이스 크기

Antibody Layer는 여러 호스트가 갖고 있는 데이터베이스에서 중복성을 제거하고, signature를 여러 host에 나누어 갖는 방식을 사용하고 있다. 즉, 각 host들은 동일한 보안계층 구조를 가지고 있지만 서로 다른 작은 크기의 데이터베이스를 가지게 된다. 이는 각 호스트에 전체 데이터베이스를 분배하는 방식으로, 한 호스트가 가지는 데이터베이스는 그 크기가 작더라도 공동검색과 Antigen에 대한 정보교환으로 그룹 내의 호스트들에게는 그룹 전체가 가지고 있는 데이터베이스를 이용한 보안수준이 제공된다. 따라서 Host alliance 그룹에 참여한 호스트들은 작은 데이터베이스만을 가지고 있더라도 Antigen의 Detection에 정확도와 효율성을 동시에 만족할 수 있게 된다.

· Antigen의 확산

Antibody Layer[1]에서 각 호스트들이 가지고 있는 데이터베이스 (Threat Information Bank)는 BIB(Basic Information Bank)와 EIB(Evolved Information Bank)의 두 가지가 있다. BIB는 호스트들간에 공유되는 단순검색을 위한 데이터베이스로 자발적인 대처능력을 가지도록하고 있으며, EIB(Evolved Information Bank)는 다변화된 항체 정보들이 생성·저장된다. EIB는 호스트들간에 공유되지 아니하고 공동검색 요청에 검색결과만을 응답하여 주게 되는데, EIB는 동일한 인터넷 항원에 대해서도 호

스트마다 서로 다른 검색결과를 만들 수 있으므로 EIB에서 Antibody Layer의 다양성이 나타나게 된다. 즉, 다변화된 시스템에 의해 한 시스템이 공격을 받더라도 같은 공격법에 의해서 다른 시스템이 공격당할 확률이 줄어들게 된다[2]. 따라서 다양성을 통해 Antigen의 확산을 효과적으로 막을 수 있다.

2.3 Cooperation Protocol

Antibody Layer는 데이터 베이스의 분산성과 검색의 다양성을 갖기 위해, Host alliance 그룹을 형성하고 그룹 멤버간에 데이터베이스 공유와 공동검색을 하게 되며, Cooperation Protocol은 이러한 그룹내의 호스트들간의 커뮤니케이션을 위한 수단을 제공하고 있다. Host alliance 그룹의 분산되어있는 데이터 베이스의 규모는 적절한 보안 수준을 제공하기 위한 크기가 되어야 하지만, 각각의 host들은 자원의 상태에 따라 매우 작은 크기의 데이터 베이스를 가질 수 있으므로 그룹의 멤버수는 상당히 커질 수도 있다. 따라서, Cooperation Protocol은 효율적인 그룹 커뮤니케이션을 위해 멀티캐스트를 사용하게 된다.

Antibody Layer[1]에서는 상호 정보교환을 위해 기본적인 공동검색 프로토콜을 제시하고 있으며 다음과 같다.

· 가정

그룹 커뮤니케이션을 위해 필요한 Secure, Authentication등의 보안서비스를 제공하는 Secure Multicast Channel이 설치되어있다.

· Message Notations

REQ(REQUEST) : 공동검색 요청

ANT(ANTIGEN) : 인터넷 항원 경고 메시지

· 공동검색 프로토콜

i. 호스트가 REQ를 전송한다(그림 3-(a)).

ii. 면역 네트워크 그룹멤버 (Alliance)는 REQ를 받아 각자 검색을 수행(그림 3-(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 3-(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.

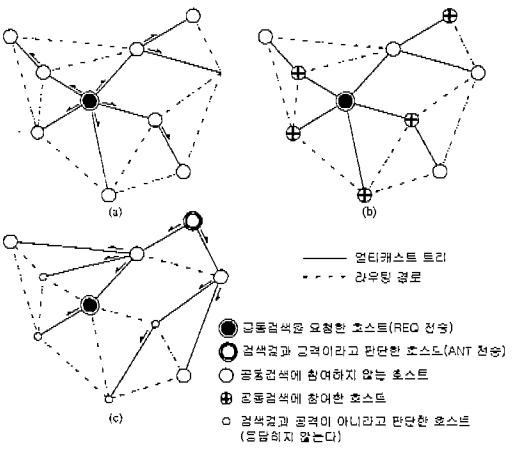

그림 3. 공동검색 요청을 따른 면역네트워크 그룹의 작용. (a) 공동검색 요청을 멀티캐스트. (b) 면역네트워크 그룹 멤버는 요청을 받아 각자 검색을 수행. (c) 공격이라고 판단한 호스트는 이를 멀티캐스트

Cooperation의 과정은 Host alliance 그룹내의 검색을 요청한 호스트(initiator)가 Cooperation을 시작하고 그룹 멤버들이 검색을 종료한 후에 검색결과를 응답하기까지를 의미한다. Cooperation은 그룹 멤버중 누구라도 요청할 수 있으며 다른 멤버들(requestees)은 이 요청에 대해 공동검색을 수행한다. 따라서, 검색요청이 매우 빈번하게 일어날 경우 각 멤버들의 시스템 리소스는 검색요청에 의해 많이 소모되는 것이 당연하므로 Cooperation 수행에 대한 Coordination을 해야 한다. 이때 중요한 파라미터들은 다음과 같다.

- Inter-request interval (request rate)
- Group size
- Request data size
- Member bank size
- Maximum scanning time

Inter-request interval은 그룹의 크기와 각 멤버의 데이터베이스(information bank)의 크기에 따라서 제한된다. 따라서 한 Host의 평균적인 Inter-request interval을 고려할 때 그룹 전체의 효율이 유지되는 한도내에서 최대 멤버수와 Maximum bank size를 설정해야한다. Maximum scanning time은 Host가 해당 요청에 의한 검색에 걸리는 최대 시간이므로 Host의 가능한 리소스 양이나 Bank size에 따라서 Host들의 검색시간의 분산을 최소화해야 한다.

공동검색을 요청하는 Initiator가 보내는 요청 메시지(REQ)는 다음의 정보를 포함한다.

REQ Message Format
- Requester_ID
- Group_ID
- Data chunk
- Diversity Vector (DIV)

Requestee는 자신의 리소스에 따라 cooperation에 참가할지 결정하게 되며 Cooperation에 참가한 호스트는 자신의 데이터베이스를 가지고 Data chunk가 Antigen인지를 판단한다. Basic Antibody Layer와 Evolved Antibody Layer의 결과 값은 검색을 수행한 데이터가 Antigen으로 판단될 경우 ANT(Antigen)가 되며, 이러한 판단결과는 호스트 자신의 데이터 베이스를 업데이트하고 그룹 전체에 보내져 다른 호스트들의 데이터베이스를 업데이트하는데 이용된다. 만약, 공격이 아니라고 판단된 경우에 Antibody Layer는 검색결과로 Negative signal을 출력하고, 이를 cooperation session이 종료하는 시점을 판단하는데 사용할 수 있다. 하지만 공동검색의 요청에 대한 응답 속도는 호스트마다 다를 수 있으므로 응답이 한번에 몰리는 경우 문제가 될 수 있다. 그래서 그림3-(c)에서와 같은 응답 억제(response suppression) 알고리즘을 사용한다.

따라서 Session의 종료 시점의 판단을 위해서는 REQ 메시지의 DIV로부터 얻어낸 각 호스트간의 단대단 최대 전송지연, 호스트 리소스, 데이터베이스 크기 등에 의해 미리 설정된 타이머를 이용하게 된다. 실시간 Antigen detection을 위해서 타이머가 종료하기 전에 검색이 종료되어야 하므로 DIV의 파라미터들이 적절하게 설정되어야 한다.

Diversity Vector(DIV) Format
- Bank size
- Mean scanning time
- Environment (OS, H/W, S/W, etc.)

III. 결 론

Antibody Layer는 네트웍에 연결된 호스트들 간의 상호 정보교환과 고도의 병렬처리에 의해 궁극적으로 디지털 면역 네트웍을 형성하고자 제안되었으며, 본 논문에서는 이러한 Antibody Layer특징을 살펴보고 정보교환과 병렬처리의 중요한 메커니즘인 Cooperation Protocol을 살펴보았다. 특히, Cooperation Protocol에서 고려되어야할 파라미터들에 대하여 논하였다. Cooperation Protocol의 완성을 위해서는 시뮬레이션을 통한 최적화된 파라미터 설정이 선행되어야 한다.

감사의 글 : 본 연구는 한국산업자원부 2000년 제2차 산업기반기술 개발사업(공통핵심/Spin-Off)의 연구비지원으로 수행되었으며 연구비 지원에 감사드립니다.

IV. 참고문헌

[1] Jabeom Gu, Dongwook Lee, Kweebo Sim and Sehyun Park, *Antibody Layer for Internet Security,* GLOBECOM 2000. IEEE , Volume: 1 , 2000 Page(s): 450-454

[2] Anil Somayaji, Steven Hofmeyr, Stephanie Forrest, *Principles of a Computer Immune System,* 1997 New Security Paradigms Workshop Langdale ,1998

[3] Dipankar Dasgupta, *An Overview of Artificial immune systems and Their Applications,* Artificial immune systems and Their Applications Part I , Springer, 1998, Page: 3-18,

[4] Charles Janeway, Paul Travers, J. donald Capra, Mark J. Walport, *Immunobiology: The Immune System in Health and Disease,* 1999