Proceedings of KFIS 2001 Spring Conference, 2001. 5. 19

인터넷 보안을 위한 디지털 면역 네트워크

Digital Immune Network for Internet Security

한국민, 구자범, 심귀보, 박세현
중앙대학교 전자전기공학부

Kukmin Han, Jabeom Gu, Kweebo Sim and Sehyun Park
School of Electrical and Electronic Engineering, Chung-Ang University
E-mail : ankh@wm.cau.ac.kr

ABSTRACT

기존의 침입 탐지 시스템(Intrusion Detection System)은 점점 복잡해져 가는 네트워크, 다양화되고 지능화되는 해킹 기술과 바이러스의 공격으로부터 시스템을 보호하기 위해 처리해야 하는 정보의 양과 복잡한 알고리즘으로 인해 실시간 서비스의 구현이 힘들다는 문제점이 있다. 본 논문에서는 시스템, 네트워크 리소스의 효율적인 분배를 통해 실시간으로 침입자를 탐지할 수 있는 네트워크 토폴로지 즉, 디지털 면역 네트워크(Digital Immune Network, DIN)를 제시한다. DIN은 침입의 탐지를 위하여 생체 면역 시스템의 B세포, T세포 개념의 알고리즘이 적용되고, 견고성 향상을 위해 메쉬 네트워크 구조가 적용되어 호스트 연합(Host Alliance)을 구성함으로써 호스트들의 병렬처리를 통해 리소스 낭비를 막고 실시간 서비스가 제공될 수 있도록 하였다.

Key words : 디지털 면역 네트워크, 생체 면역 시스템, 침입 탐지 시스템, 호스트 연합, 메쉬 네트워크

I. 서 론

최근에 인터넷을 통한 해킹이나 바이러스 침투로 인한 피해 사례들이 증가하고 있다. 2000년 2월, 야후, 아마존, CNN에 발생했던 DDoS(Distributed Denial of Service) [2, 3, 4] 공격으로 인해 각 웹사이트들은 큰 피해를 입었다. 야후의 경우 초당 기가비트의 서비스 요청으로 인해 무려 3시간 이상동안 서비스가 중지되는 사태로 우리에게 방화벽이나 침입 탐지 시스템의 필요성을 부각시켜 준다. 이렇게 인터넷의 개방성은 사용자들에게 매우 다양한 서비스를 제공하는 반면에 인터넷을 통한 해킹, 바이러스등의 공격을 위한 도구로서 이용되고 있다. 이러한 문제점에 대한 해결책으로 지난 20여년간 방화벽이나 암호화 등의 access control 방법이 연구 되었고, 90년대 이후로 access control이 해결하지 못한 문제점은 침입 탐지 시스템을 통해 해결하려는 노력이 진행되어 왔다. 본 논문에서는 지금까지 연구된 침입 탐지 시스템을 소개하고 기존의 침입 탐지 시스템의 문제점이 무엇이며, 이를 해결하기 위해 생체 면역 시스템의 알고리즘이 적용된 네트워크 토폴로지, 즉 디지털 면역 네트워크를 제시한다.

II. 본 론

2.1 침입 탐지 시스템

침입(Intrusion)이란 비 인가된 사용자가 자원의 무결성, 기밀성, 가용성을 저해하는 일련의 행위들로 정의될 수 있다. 침입 탐지 시스템은 침입과 자원의 오용을 탐지하고 방어하는 시스템이다.

지금까지 인터넷을 통한 해킹, 바이러스, DoS 공격 등을 탐지하고 방어하기 위한 노력으로 많은 침입 탐지 시스템의 prototype이 연구되고 개발되어 왔다. 침입 탐지는 크게 침입 자료에 의한 분류와 침입 행위에 의한 분류

로 나뉘어 질 수 있다. 먼저, 침입 자료에 의해 호스트 기반(Host-based), 네트워크 기반(Network-based) 침입 탐지로 분류되고, 침입 행위에 따라 비정상적 침입 탐지(Anomalous Intrusion Detection)와 오용 침입 탐지(Misuse Intrusion Detection)로 분류된다.

2.1.1 침입 자료에 의한 분류

호스트 기반 침입 탐지 시스템 (Host-based Intrusion Detection System)[1]은 호스트 OS의 감사자료를 주된 입력 정보로 하여 침입자를 탐지하는 시스템으로써 현재 침입 탐지 시스템의 대부분을 이룬다. 프로그램, 프로세스 변수, OS의 log 정보 등의 감사자료를 수집하여 호스트 내부에서 정해진 이상의 억세스 권한을 얻으려는 사용자의 수상한 행동을 탐지하고 오용의 여부를 판단한다. 네트워크 기반 침입 탐지 시스템(Network-based Intrusion Detection System)[1]은 네트워크 상에 흐르고 있는 패킷들을 수집해서 프로토콜을 해석하여 감사자료로 사용하는 침입 탐지 시스템이다. 이 시스템은 호스트 기반 시스템과 같은 알고리즘을 적용하여 네트워크에 연결되어 있는 여러 호스트들의 감사자료를 중앙의 호스트로 전송하고 중앙의 호스트는 이 정보들을 처리하여 여러 호스트들의 트래픽을 감시하게 된다.

2.1.2 침입 형태에 의한 분류

비정상적 침입 탐지 시스템(Anomalous Intrusion Detection System)[1]은 컴퓨터 자원의 비정상적인 행위에 근거하여 미리 정의된 모델을 이탈할 경우 침입으로 간주하는 시스템이다. 이것은 과거의 경험적인 비정상적인 침입의 탐지를 통계적으로 처리하는 방법, 경험적인 특정 침입 패턴의 집합을 설정하여 침입을 분류하고 예측하는 방법, 여러 가지 비정상적인 행위 측정 방법들을 사용하여 각각의 결과를 통합하여 침입을 측정하는 방법, 명령어의 순서를 신경망을 통하여 학습시켜서 다음에 수행될 명령을 미리 예측하는 방법 등을 이용하여 구성될 수 있다. 오용 침입 탐지 시스템(Misuse Intrusion Detection System)은 시스템이나 응용 소프트웨어의 취약성을 이용한 침입을 탐지하는 시스템이다.

2.2 기존 침입 탐지 시스템의 문제점

기존의 침입 탐지 시스템을 이용해서 점점 복잡해져 가는 네트워크, 다양화되고 지능화되는 해킹 기술과 바이러스의 공격으로부터 시스템을 보호하기에는 공격 패턴에 대한 많은 정보의 양과 알고리즘의 복잡성으로 인해 효율적 유용 시간 내 침입 탐지가 가능하지 않다. 더욱이 본 연구실에서 진행중에 있는 보안항체 계층(Antibody Layer)[5]과 인공 면역 시스템의 알고리즘에 관한 연구가 적용될 경우 알려지지 않은 형태의 침입까지도 탐지가 가능하지만 이에 대한 정보는 한 호스트가 감당할 수 없는 양이 된다. 그리고 기존 침입 탐지 시스템의 대부분은 호스트 기반 침입 탐지 시스템과 같은 단일 호스트의 보호에만 국한되어 있는 시스템이기 때문에 DDoS 공격의 예에서처럼 한 핵커에 의해 조종 받고 있는 좀비(Zombie) 컴퓨터로부터의 분산된 공격에 대해서는 지역적이고 일시적인 해결책일 뿐, 근본적인 해결책은 될 수 없다. 한 호스트를 대상으로 하는 집중적인 공격은 방어가 되었다 하더라도 트래픽의 증가로 주변 네트워크는 정체 현상을 일으켜 QoS를 보장 받을 수 없게 되고, 공격이 다른 호스트로 퍼져 나가는 것을 예방 할 수도 없다. 이와 같은 공격에 대해서는 호스트들이 연합을 구성함으로써 좀비 컴퓨터를 탐지하여 그 정보를 서로 공유하고 방어할 수 있는 전체적인 보안 네트워크 체계가 필요하다.

이러한 기존의 침입 탐지 시스템의 문제점을 해결하기 위해 본 논문에서 디지털 면역 네트워크(Digital Immune Network)를 제시한다.

2.3. 디지털 면역 네트워크

2.3.1 디지털 면역 네트워크의 특징

디지털 면역 네트워크(Digital Immune Network, DIN)는 기존 IDS의 효율을 높여 네트워크에 연결된 호스트들간의 상호 정보 교환과 고도의 병렬처리를 통해 실시간 서비스가 유지될 수 있도록 한다. 해킹이나 바이러스가 인터넷을 기반으로 퍼지고 있는 것과 마찬가지로 DIN 역시 인터넷을 기반으로 그 보안 영역을 형성하기 때문에 컴퓨터 보안에 최적의 해결책이 될 수 있다.

DIN은 기존의 IDS에 비해 다음과 같은 장점을 가지고 있다.

- DIN의 보안 서비스를 이용하여 시스템 리소스가 적은 호스트도 동일하게 높은 수준의 보안 서비스를 받을 수 있다. PDA등과 같이 시스템 리소스가 적은 호스트는 자신이 직접 검색을 하지 않고 호스트 연합에 의해 구성된 보안 그룹에 검색을 요청하여 그 결과만을 받아서 처리할 수 있다.
- 공격의 확산 방지에 유리하다. 최근 바이러스가 e-mail을 통해 확산되는 등

인터넷을 통한 감염이 증가하고 있다. 이런 예들은 감염의 확산을 방지하는 것이 얼마나 중요한지를 단적으로 보여준다. 호스트 연합은 네트워크에서 호스트 들끼리의 지속적인 정보교환이 일어나므로 인터넷을 통한 감염에 신속하게 대처할 수 있다.

- 새로운 바이러스를 검색하는 것은 시간과 자원이 많이 소요되는 작업이므로 호스트 연합에서의 병렬처리를 통하여 리소스 낭비를 막고 실시간의 서비스를 제공할 수 있다.

DIN은 기존의 침입 탐지 시스템을 기반으로 하지만, 생체 면역 시스템의 B세포, T세포 개념의 알고리즘과 메쉬 네트워크 구조를 적용하여 전체적인 보안 네트워크 체계를 형성한다.

2.3.2 생체 면역 시스템

생체 면역 시스템의 기본 요소는 B세포와 T세포이다[6]. B세포는 생체에 침입하거나 들어온 외부 물질인 항원에 대항해 항체를 분비함으로써 항원을 제거하는 역할을 한다. T세포는 B세포를 활성화시켜 항체의 분비를 촉진하는 역할을 하는 보조 T세포(Helper T-cell)와 항원에 의해 감염된 자기세포를 식별하여 죽이는 역할을 하는 세포독성 T세포(Cytotoxic T-cell), 그리고 항체에 의한 면역 시스템이 활성화 된 이후 시스템을 억제하는 역할을 하는 억제 T세포(Suppressor T-cell)로 구분된다.

이러한 생체 면역 시스템의 B세포, T세포 개념을 적용한 알고리즘은 외부에서 침입한 항원(해킹, 바이러스 등)을 제거하고, 항원에 의해 감염된 세포(응용 프로그램 등)를 제거하는 역할을 한다.

그림 1은 T세포가 어떻게 유추작업을 통해 처방을 생성하는지를 보여준다. 각 T세포는 이미 알려진 항원의 처방에 관한 정보를 공유하고 있고 새로운 항원에 대한 자신만의 처방 정보를 가지고 있다(그림 1(a)). 그림 1(b)에서는 어떻게 T세포가 알려진 처방과 자신만의 처방 정보를 조합해서 새로운 처방을 생성하는지를 보여준다. 새로운 처방이 생성되면 T세포는 다른 T세포와 정보를 공유한다(그림 1(c)).

2.3.3 메쉬 네트워크 (Mesh Network)

메쉬 네트워크 구조를 기반으로 DIN의 견고성(robustness)은 더욱 향상될 수 있다. 견고성의 향상을 바탕으로 호스트 연합이 안정된 접속망 상에서 구성되고 호스트들끼리 네트워크를 통해서 서로 항원과 처방에 대한 정보를

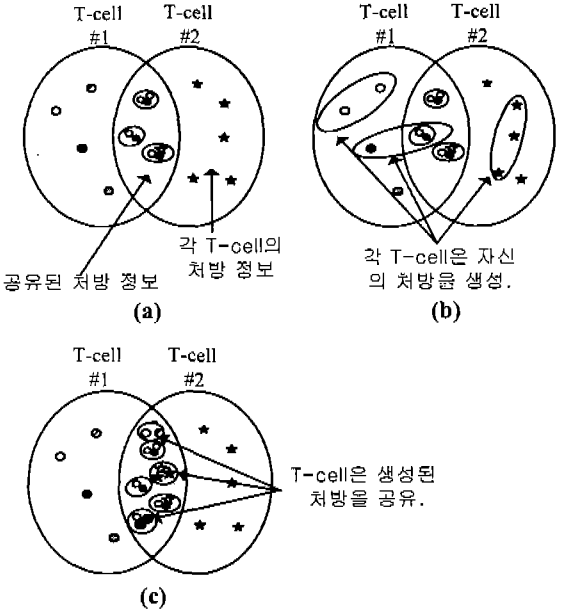

그림 1. T세포의 유추작업을 통한 처방 생성 과정
(a) 각 T세포는 자신만의 처방 정보와 공유된 정보를 가진다. (b) 각 T세포는 두 T세포의 공유정보를 통해 새로운 처방을 생성한다. (c) T세포는 생성한 새로운 처방을 다른 T세포와 공유한다.

교환하고 협력한다. 이러한 정보들이 DIN을 통해 공유되어 언제든지 새로운 항원에 대한 해결책을 다른 호스트에 요청할 수 있고, 여러 호스트들의 분산처리를 통하여 빠르고 효율적으로 항원을 탐지하고 처리할 수 있게 된다.

2.4 DDoS 공격에 대한 DIN의 효율성

DDoS 공격은 공격자가 분산된 좀비 컴퓨터를 두어 목적 호스트를 동시에 공격함으로써 시스템 리소스를 고갈시킨다. 이러한 공격은 공격자를 찾아내거나 분산되어 있는 좀비 컴퓨터를 찾아내서 제거하지 않는 한 근본적인 해결책이 될 수 없다. DIN에서는 호스트 연합이 구성되어 각 호스트들끼리 정보를 교환하고 공유함으로써 분산된 좀비 컴퓨터를 찾아내고 방어하는데 근본적인 해결책이 될 수 있다.

그림 2는 DIN에서 DDoS 공격을 방어하는 모습을 보여준다. 그림 2(a)는 호스트 연합이 구성되어 있지 않은 경우에 공격 대상 호스트 근처에 있을 수 있는 좀비 컴퓨터와 DDoS 공격 경로가 나타나 있다. 호스트 연합이 구성되어 있는 경우에는 호스트 연합 내의 좀비 컴퓨터가 제거되고(그림 2(b)), 호스트 연합 외부로부터의 DDoS 공격은 호스트 연합 멤버들에 의해 차단되어 공격 대상 호스트는 공격으로부터 보호 된다. (그림 2(c)).

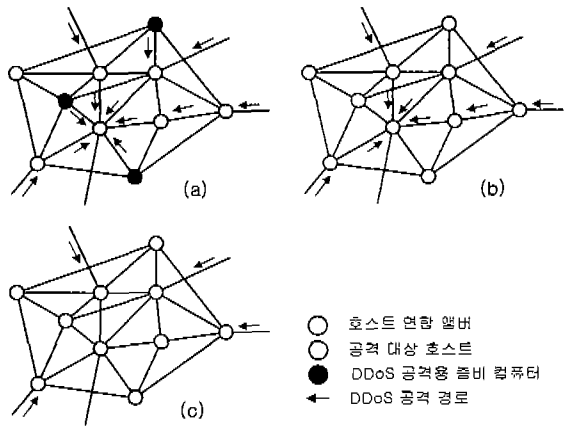

그림 3은 호스트 연합에 의해 DDoS 공격이 어느 정도 차단되었지만 다른 경로를 통한 공격으로 시스템 및 네트워크 자원이 고갈되어 더 이상 서비스를 할 수 없는 상태를 보여준다. 이를 위해 DIN에서는 메쉬 구조의 네트워크를 이용하여 지원 가능한 호스트 연합 멤버로부터 대체 경로를 통해 서비스를 받음으로써 통신의 QoS를 보장할 수 있다.

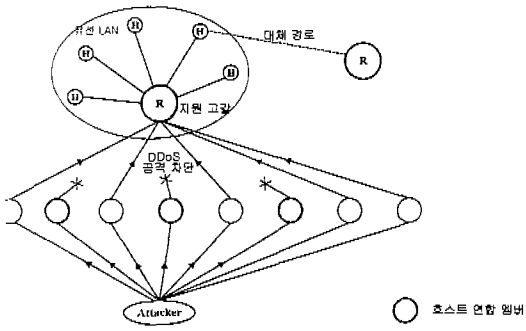

그림 3. DIN에서의 DoS 공격 차단 및 Mesh network에 의한 대체 경로

III. 결 론

본 논문에서는 지금까지 연구된 침입 탐지 시스템에 대해서 소개하였고, 기존의 침입 탐지 시스템은 어떤 문제점이 있는가를 제시하였다. 특히 DDoS 공격에 대해서는 일시적이고 지역적인 해결책만을 제시할 수 있을 뿐, 근본적인 해결책은 될 수 없었다. 그러나 본 논문에서 제시한 디지털 면역 네트워크는 메쉬 네트워크 구조의 견고성 향상을 통하여 호스트 연합을 구성하고 그 멤버들은 항원과 처방에 대한 정보의 공유와 병렬처리로 외부에서 침입한 항원에 대해 빠르고 효과적으로 대처할 수 있다. 각 호스트의 침입 탐지 시스템은 생체 면역 체계의 알고리즘을 적용함으로써 B세포 과 T세포들의 호스트 연합을 통해 항원에 대한 방어의 효율성을 높일 수 있다.

앞으로는 생체 면역 체계를 컴퓨터 네트워크에 적용하는 효과적인 알고리즘과 호스트 연합에 필요한 프로토콜을 구현하는 연구가 수행되어야 할 것이다.

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

IV. 참고문헌

[1] Biswanath Mukherjee, L. Todd Heberlein, and Karl N. Levitt, "Network Intrusion Detection", IEEE Network, Volume: 8 Issue: 3, May-June 1994, Page(s): 26 -41

[2] Felix Lau, Stuart H. Rubin, Michael H. Smith, Ljiljana Trajkovic, "Distributed Denial of Service Attacks", Systems, Man, and Cybernetics, 2000 IEEE International Conference on, Volume: 3, 2000, Page(s): 2275 -2280

[3] Xianjun Geng and Andrew B. Whinston, "Defeating Distributed Denial of Service Attacks", *IT Professional*, Volume: 2 Issue: 4, July-Aug. 2000, Page(s): 36 -42

[4] John Elliott, "Distributed Denial of Service Attacks and the Zombie Ant Effect", *IT Professional*, Volume: 2 Issue: 2, March-April 2000, Page(s): 55 -57

[5] Jabeom Gu, Dongwook Lee, Kweebo Sim and Sehyun Park, "An Antibody Layer for Internet Security", Global Telecommunications Conference, 2000. GLOBECOM '00. IEEE, Volume: 1, 2000, Page(s): 450 -454

[6] 심귀보, "컴퓨터 면역시스템 개발을 위한 생체 면역시스템 모델링", 한국퍼지 및 지능시스템학회 논문집, 2000. April, Volume: 10, No.2