차세대 네트워크 환경에서의 보안 인프라 구축을 위한 새로운 전략

중앙대학교 구자범 · 박세현*

1. 서 론

최근 인터넷을 통해 행해진 DDoS 공격과 인터넷 웜의 확산은 위협이 위험 수위가 점점 높아지고 있고, 향후의 공격 방법은 점점 다양화되고 복잡한 형상으로 발전하여 더욱더 많은 피해를 줄 것으로 예상된다[1]. 특히 이동통신 네트워크 기술의 발전에 힘입어 유비쿼터스 컴퓨팅과 같은 이질적 네트워크 환경에서 수많은 이동 단말이 이러한 위협에 그대로 노출될 것으로 예상된다.

현재 개별 호스트나 지역 망에 적용되고 있는 방화벽, 침입 차단 시스템, 침입 탐지 시스템, 취약성 분석 시스템 및 바이러스 백신 등의 보안 시스템들은 DDoS와 같이 분산 협력 방식으로 다양하고 복잡하게 진화하는 공격에 효과적으로 대응할 수가 없고, 인터넷 웜의 빠른 확산에 적절히 대응하지 못하고 있다. 이러한 주요 원인은 이들 정보 보호 시스템들이 네트워크 차원에서 효율적이고 적극적인 대응이 불가능하며, 새로운 공격 패턴이나 보안 정책 등의 변화에 적응이 어려운데 기인한다. 따라서 이러한 문제점을 해결하기 위하여 다양한 공격에 대해 능동적 대응이 가능하며, 보안 시스템들간에 협업을 통한 광역망 차원의 보안 기능을 제공하고, 사용자의 요구에 따라 보안 정책의 다변화가 용이한 보안의 새로운 구조가 필요하다. 본 논문에서는 현재의 네트워크 뿐만 아니라 유비쿼터스 환경과 같은 차세대 이동 네트워크 하에서 이질적 시스템을 위한 새로운 보안 전략인 면역 네트워크에 대해 논의한다.

본 논문은 다음과 같이 구성된다. 2장에서는 다양해지는 공격 방법과 차세대 네트워크의 환경 변화에 대해 논의하고, 3장에서는 본 논문에서 면역 네트워크의 개념과 주요 구성 요소에 대해 논의하고, 4장에서 결론을 맺는다.

* 종신회원

2. 공격 방법 및 환경의 변화

2.1 공격 방법의 진화

현재 운영되고 있는 방화벽, 침입 탐지 시스템, 바이러스 백신 등의 보안 시스템은 개별 호스트를 대상으로 하거나 지역 망을 외부 망으로부터 보호하기 위한 기능을 제공하고 있다. 그러나 이들 보안 시스템은 다른 호스트나 네트워크간의 상호 연관관계를 알기 어렵고 이상 징후 탐지시 이를 종합적으로 판단하는 것이 불가능하다. 또한 탐지된 공격에 대한 대응이 개별 호스트에서 독자적으로 이루어질 수 밖에 없어 효율적인 대응을 기대할 수 없다.

이들 보안 시스템은 '알려진 공격에 대한 탐지 및 대응' 부분에서는 탁월한 성능을 발휘하고 있지만, 최근 네트워크를 기반으로 이루어진 다양한 DDoS 공격과 인터넷 웜의 확산은 '진화'라고 일컬어질 만큼 그 종류와 방법이 다양해지고 있어, 현재의 보안 시스템이 끊임없이 진화하는 공격 방법에 적극적이고 실시간으로 대응하는 것은 불가능하다[2][3].

최근에는 외부 침입체(antigen)에 대한 생체 면역 시스템의 탐지/대응 기법을 컴퓨터 네트워크에 적용하려는 연구가 진행되고 있어, 진화하는 공격 방법에 대한 대응책으로 관심을 모으고 있다[4-6]. 특히 생체 면역 시스템에서 T-Cell(탐지), B-Cell(대응) 등 세포 작용[7]은 컴퓨터 네트워크에서의 웜이나 해킹과 매우 유사하다고 할 수 있는데, [6] 에서는 생체 면역 시스템을 모델로 하여 진화하는 공격 방법에 대응하기 위해 보안 시스템이 갖추어야 할 기본 사항을 다음과 같이 기술하고 있다.

- **분산된 탐지 기법(Distributability)** : 침입체에 대한 탐지는 분산된 호스트에서 이루어져야 하며, 중앙 집중의 관리 방식은 단일 장애점(SPOF: Single Point of Failure)을 없애는 측면에서 바람직하지 않다. 이것은 전체 네트워크 관점 분산된 공격 탐지가 요구됨을 의미하고 있다. 본 논문에서는 이러한 분산된 보안 시스템을 구성하기 위한 방안을 논의한다.
- **다층 구조(multi-layered)** : 공격 탐지 및 대응의 성공 가능성을 높이기 위해서는 여러 가지 보안 기술을 동시에 적용하는 것이 필요하다. 침입 탐지 등의 분야에서는 이미 이 사항의 중요성을 인식하여 다양한 탐지 기술을 통합하여 사용할 것을 권하고 있다. 그러나 다층 구조를 적용할 대상이 이동 단말이라고 한다면, 부족한 시스템 자원으로 인해 효율적인 탐지가 불가능 할 수밖에 없다. 본 논문에서는 다양한 시스템에 적용 가능한 새로운 보안 시스템의 전략에 대해 논의한다.
- **다변성(diversity)** : 다변성은 생체 면역 시스템과 매우 밀접한 연관이 있다. 생체 면역 시스템에서 설명된 다변성은 생체학적인 탐지 기법의 다변성을 의미하며, 다변화된 세포에 의해 탐지 가능성을 높인다는 것이다. [6]에서는 이러한 다변성을 다음과 같이 설명하고 있다. 즉 시스템이 다변화된다면, 한 시스템이 공격을 받더라도, 같은 공격법에 의해서 다른 시스템이 공격당할 확률을 줄일 수 있는 것이다. 따라서 침입체의 확산을 막을 수 있는 기반을 형성할 수 있다는 의미이다. 그러나 다변성을 실제 네트워크 환경에서 기대하기는 매우 어렵다. 비록 유비쿼터스 환경의 이질적인 네트워크라고 하더라도, 생체 면역 시스템에서 세포 분열에 의해 이루어지는 다변성을 컴퓨터 시스템에서 구현하는 것이 불가능하기 때문이다. 본 논문에서는 다변성에 대해 분산 네트워크 상에서 공격 탐지의 효율성을 높이기 위한 새로운 방안으로 이용하고 있다.

2.2 환경의 변화

차세대 네트워크는 크고 작은 다양한 플랫폼 상에서 이질적 특징을 갖는 이동 단말이 능동적 통신을 형성하는 구조라고 할 수 있어 매우 복잡한 네트워크 구조가 될 것으로 예상된다[8-11].

차세대 네트워크의 특징 중 네트워크 및 시스템 보안에 중대한 영향을 미치는 요소들은 다음과 같다.

- 네트워크를 구성하는 단말 및 호스트의 이질성 증가로 인해 하나의 보안 시스템을 전체 호스트에 일괄적으로 적용하기가 매우 어렵다.
- 이동 네트워크의 All-IP 구조 채택에 의한 네트워크의 복잡성 증가로 인해 기존의 유선망에서 존재하던 다양한 공격 기법이 All-IP 구조의 이동 네트워크에도 그대로 적용된다.
- 복잡해진 네트워크로 인해 중앙 집중적 관리가 불가능하고, 언제 어디에서나 접속 가능한 개방성으로 인해 방화벽과 같이 지역망을 외부망으로부터 단절하는 방식의 보안 시스템이 효능을 발휘하기 어렵다.
- 이동 사용자 지역망으로 이동할 경우 이에 대한 관리가 불가능하므로 네트워크 관리 체계가 모호해지고 일괄적인 보안 정책을 적용하기가 어렵다.

이러한 특징 중 특히 이동 사용자가 지역망으로 이동하여 지역망을 자유롭게 사용하는 것은 가장 큰 문제점이라고 할 수 있다. 외부로부터 지역망으로 이동해온 사용자는 지역망과 신뢰관계가 성립되어 있지 않은 경우가 대부분이다. 또한 사용자는 바이러스나 해킹 등의 공격에 침해당한 후 또 다른 공격의 종속 매체로 동작하거나 사용자 스스로 공격을 시도할 수 있으므로 잠재적으로 위협적인 요소를 갖고 있다고 할 수 있다. 이러한 사용자가 지역망으로 이동해 들어오는 경우 이동 사용자 자체가 보안 취약 요소로 작용할 수 있어 로컬 네트워크 내부에서의 분산 공격, 데이터 유출, 백도어 설치 등의 악영향을 초래할 수 있는 가능성이 높아진다.

차세대 네트워크의 개방성은 사용자들에게 매우 다양한 서비스를 제공하는 반면, 이러한 개방성에 기반한 공격 방법은 점점 다양화되고 복잡한 형상으로 발전할 것으로 예상되어 이질적 네트워크 환경에서 수많은 이동 단말이 새로운 위협에 그대로 노출될 것으로 예상된다. 따라서 본 논문에서는 차세대 네트워크 보안을 위한 새로운 보안 전략을 제시한다.

3. 새로운 보안 전략

본 논문에서는 차세대 네트워크 환경에서 네트워크와 이동 단말의 시스템 리소스, 자유로운 이동성 등의 새로운 환경 변화와 다양하고 복잡한 네트워크

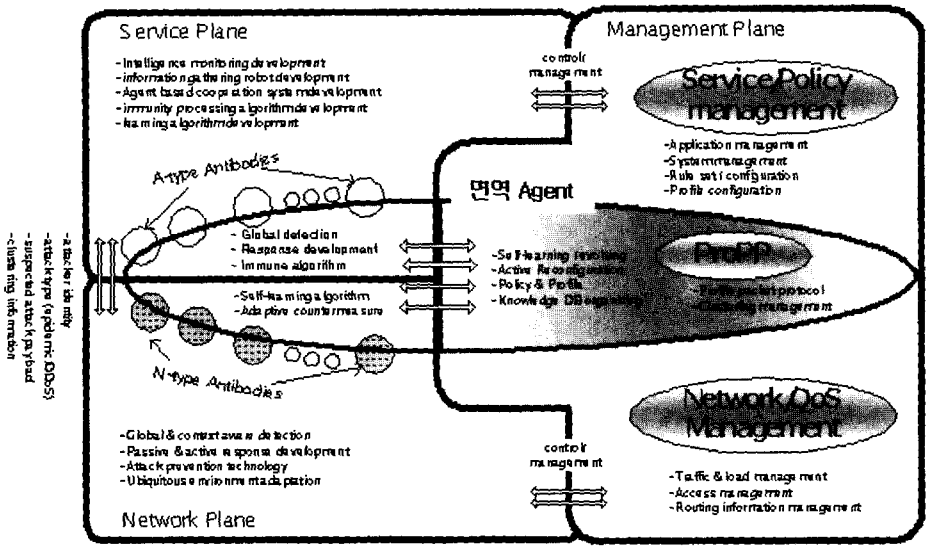

그림 1 서비스, 네트워크, 관리 분야에서의 면역 agent 역할

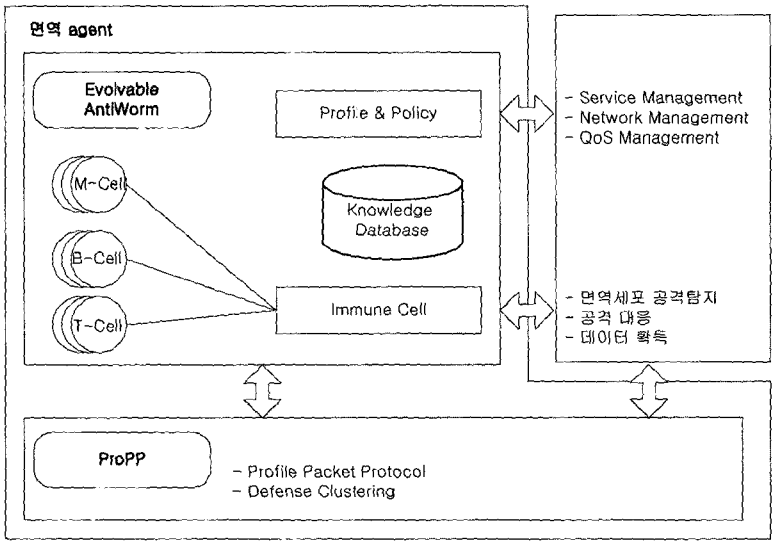

그림 2 면역 agent의 구성 요소

구조에서 기존의 대응 방안이 갖는 문제점을 극복하고, 실시간으로 적용 가능한 새로운 대응책으로 면역 네트워크를 제안한다. 면역 네트워크는 다변화할 수 있는 면역 agent에 의해 형성되는 새로운 보안 인프라이다. 그림 1은 서비스 분야, 네트워크 분야, 관리 분야에서 면역 네트워크의 핵심 요소인 면역 agent 역할을 도시화한 것이다.

면역 agent는 시스템 보안을 위해 서비스 분야, 네트워크 분야, 관리 분야에 이르는 다양한 요구 기능을 제공한다. 응용 서비스 분야에서는 이상 징후 탐지를 위한 지능적 모니터링, 정보수집, 대응 및 지식 성장 등의 기능을 제공한다. 네트워크 분야에서는 context 기반의 탐지, 능·수동적 대응, 공격 필터링, 주위 환경과의 적응 기능을 제공한다. 관리 분야에서

는 서비스 및 정책 수립을 위한 응용 시스템 관리, 프로파일 관리와 네트워크 및 QoS 관리를 위한 트래픽 제어, 엑세스 관리 등의 기능을 제공한다.

3.1 면역 agent 공조에 의한 면역 네트워크 형성

면역 agent는 현재의 침입 탐지 시스템, 바이러스 백신 등의 보안 시스템이 확장·개선된 형태라고 할 수 있다. Agent는 호스트에 삽입되어 공격 탐지 및 대응의 주도적 역할을 수행하고 사용자 정책을 수용하기 위한 인터페이스를 제공한다. 호스트간 협업은 agent에 의해 수행되는데, 호스트에 분산되어 설치된 agent간의 탐지 정보 등을 교환하여 탐지 효율성을 높이고 실시간의 대응을 가능하게 하는 방안이다. 새로운 보안 전략의 핵심 요소인 면역 agent의 구성 요소는 그림 2와 같다.

그림 2에서 Evolvable AntiWorm은 지능형 보안 시스템을 구현하기 위한 요소로, 다양한 시스템을 위한 profile 및 policy 관리, 지식 데이터베이스, 면역 세포 기술로 구성된다. ProPP(Profile Packet Protocol)는 네트워크 공조를 위한 profile 정보 교환과 cluster 기반의 방어 시스템 구축을 위한 프로토콜이다.

3.1.1 지식 성장형 agent 구현을 위한 Evolvable AntiWorm

최상의 보안 QoS를 보장하는 면역 네트워크를 구성하기 위해서 다양한 환경 하에서 사용자의 정책 설정, 주위의 agent 등의 요소에 따라 agent가 제공하는 서비스가 결정되고, 사용자는 이러한 환경에서 적응적·능동적으로 면역 네트워크에 참여하게 된다. 또한 적응적 프로파일에 따라 context 인지형 보안 시스템이 가능하게 된다. 즉 네트워크에 행해지는 공격 형태나 이상 징후를 이용하여 보안 context를 형성하고, 이에 따라 agent간의 정보 교환시 context를 교환하여 주변 환경에 즉각적으로 대처할 수 있는 서비스를 제공한다.

각 agent에서의 보안 context 생성은 프로파일에 따라 달라지므로 자연스럽게 [6]에서 설명된 다변성을 이룰 수 있고 이것이 다변화된 지식 성장형 agent로 작용할 수 있게 된다. 지식 성장형 agent를 위한 Evolvable AntiWorm의 핵심 요소는 다음과 같다.

- **Knowledge database** : 해킹·바이러스 탐지의 기반이 되는 방대한 공격 정보 및 이상 징후를 데이터베이스화 하여 분산 관리하고, T-Cell(공격 탐지), B-Cell(공격 대응), M-Cell(자율 진화)의 면역 세포들을 이용하여 분산된 공격 정보를 통합 관리한다. 시스템의 프로파일과 정책에 의한 시스템 고유의 context를 관리한다.
- **Agent 면역세포** : Agent 면역 세포(T, B, M-Cell)에 대한 profile과 policy들을 정의하여, 이들 profile과 policy에 따라 적절한 면역 기능을 수행하게 함으로써, 공격에 효율적으로 대처가 가능하도록 하게 하는 근간이 된다. 자율 진화세포는 네트워크의 변혁과 시스템 profile에 맞추어 agent를 진화하는 요소로, 진화의 결과는 다변화된 knowledge database로 반영된다.
- **Profile & Policy에 의한 관리** : Agent의 체계적인 통합 관리가 가능하고 면역세포들이 글로벌 관리 체계에 적합한 특성을 갖고 진화하도록 하며, 각 AntiWorm들의 지역망에서의 독립적 관리와 공조 네트워크 상에서의 통합적 관리를 통해 차세대 네트워크 환경에서 안전성, 효율성, 확장성을 극대화한다.

시스템의 context는 일반 context와 보안 context로 구분되어 저장된다. 일반 context는 시스템 상태, 이동 정보, 사용자 및 네트워크 프로파일, 주위 환경 등의 정보로 구성된다. 보안 context는 네트워크 상에서 획득할 수 있는 개념적인 보안 정보의 집합으로 정의한다. 즉 호스트가 지역망에 위치해 있다고 할 때 그 주위에 있는 다른 호스트들이 갖고 있는 보안 정보, 현재 네트워크의 안전도, 현재 진행되고 있는 공격에 대한 정보 등이 보안 context를 구성한다. 네트워크와 단말은 이러한 정보를 처리함으로써 새로운 상황에 적응적으로 대처할 수 있다.

Knowledge database에 저장되는 공격 정보는 공통 정보(Common Information)와 진화 정보(Evolved Information)로 구분된다. 공통 정보는 현재 진행되고 있는 공격에 대한 정보, 최신 보안 업데이트 등에 대한 정보를 담고 있는 정보로, 시스템의 즉각적인 대응을 필요로 하는 경우가 대부분이므로 모든 호스트가 공통적으로 소유한다. 또한 실시간 대응을 위해 지역망으로 이동해 들어오는 이동 단말은 공통 정보

를 업데이트 하여 지역망 고유의 보안 환경에 적응할 수 있다. 진화 정보는 호스트에 따라 다변화되는 공격정보이다. 이 진화 정보는 호스트마다 다른 데이터베이스를 구축하게 되므로 공조에 의한 공격 탐지시 데이터베이스를 분산하여 저장하고, 이를 병렬로 처리함으로써 효율성을 높이는 효과를 가져온다.

3.1.2 면역 agent간 협업을 위한 ProPP (Profile Packet Protocol)

면역 agent는 호스트와 라우터 등 네트워크를 구성하는 모든 개체에 plug-in 되어 공격을 탐지하고 대응하기 위한 기능들을 갖추고 네트워크 기반의 보안 인프라 제공을 위한 기본 역할을 수행한다. 이들 agent들은 타 agent들과의 밀접한 상호 연관관계 하에서 이상 징후 탐지시 이를 종합적으로 판단하고 글로벌 네트워크 차원에서 대응을 이루기 위한 공조 시스템을 구성한다. 본 논문에서는 ProPP (Profile Packet Protocol)를 이러한 공조 시스템 구축의 근간이 되는 프로토콜로 정의하였다.

Agent들간의 보안 공조 네트워크 구성은 다수의 호스트나 라우터가 능동형 보안 센서로 동작하여 네트워크상의 공격이나 문제점을 스스로 진단하고(Active detection) 전체 네트워크에 정보를 제공함으로써(Reconfiguration), 신속한 공격 대응이 가능하고 추가적인 공격으로부터 네트워크 전체를 안전하게 보호할 수 있도록 하기 위한 기반이 된다. 또한 agent의 공조는 시스템 자원이 부족한 호스트도 동일하게 높은 등급의 보안 서비스를 제공받을 수 있도록 하기 위하여 그룹 기반의 병렬처리를 통하여 자원 낭비를 막고 실시간 서비스를 제공 가능하도록 한다. ProPP를 위한 주요 프로시저는 다음과 같다.

```
Collaboration_request = [
    if trigger(i) = TRUE then {
        if i ∈ common_information
            then countermeasure(i)
        else {
            req = build_request(i)
            collaborative_request(req)
            if receive_response(r)
                then r -> common_information
                countermeasure(i) }}]
Migration = [
    if migrating() = TRUE then {
        req = build_request(null)
        collaborative_request(req)  /* request
        for common information */
        if receive_response(res)
        then res -> common_information }]
Collaboration_response = [
    if receive_request(req) = TRUE then {
        if req.ctx ∈ common_information then
            res = build_response(req.ctx, CSC)
            send_response(res)
    } else if common_information_req() = TRUE
    then {
        res = build_response(common_information)
        send_response(res) }]
```

프로시저에 대한 설명은 다음과 같다. 이상 징후 등에 의해 공조에 의한 공격 탐지가 필요한 경우 이벤트(i)를 입력으로 하여 **[Collaboration_request]** 프로시저를 수행한다. 이 프로시저에서는 우선 해당 이벤트가 공통 정보에 속하는지를 검사하고, 공통 정보로 지정되어 있으면 countermeasure()를 실행한다. 그렇지 않은 경우 네트워크 공조를 요청하고 응답을 기다린다. 수신한 응답은 이벤트 정보와 함께 공통 정보로 등록한다. 지역망으로 이동한 호스트는 지역 망 고유의 환경에 적응하기 위해 공통 정보를 **[Migration]** 프로시저를 통해 획득한다. 공조에 참여하는 호스트는 공조 요청 이벤트가 발생한 경우 **[Collaboration_response]** 프로시저를 수행한다. 이 경우 각각의 호스트는 다변화하여 소유하고 있는 진화 정보를 이용하여 이벤트에 대한 응답을 생성한다.

3.1.3 면역 네트워크 브로커:SEM(Self Evolving Manager)

SEM (Self-Evolving Manager)은 통합 보안 관리 및 능동 보안 관리를 위해 면역 agent가 프로파일에 따라 진화하여 구성한 동적이고, 높은 유연성, 확장성, 안전성 및 효율성을 가지는 보안 관리자이다. 다수의 호스트나 라우터가 능동형 관리 브로커로 동작하여 네트워크상의 공격이나 문제점을 스스로 진단하고 전체 네트워크에 정보를 제공함으로써(recon-

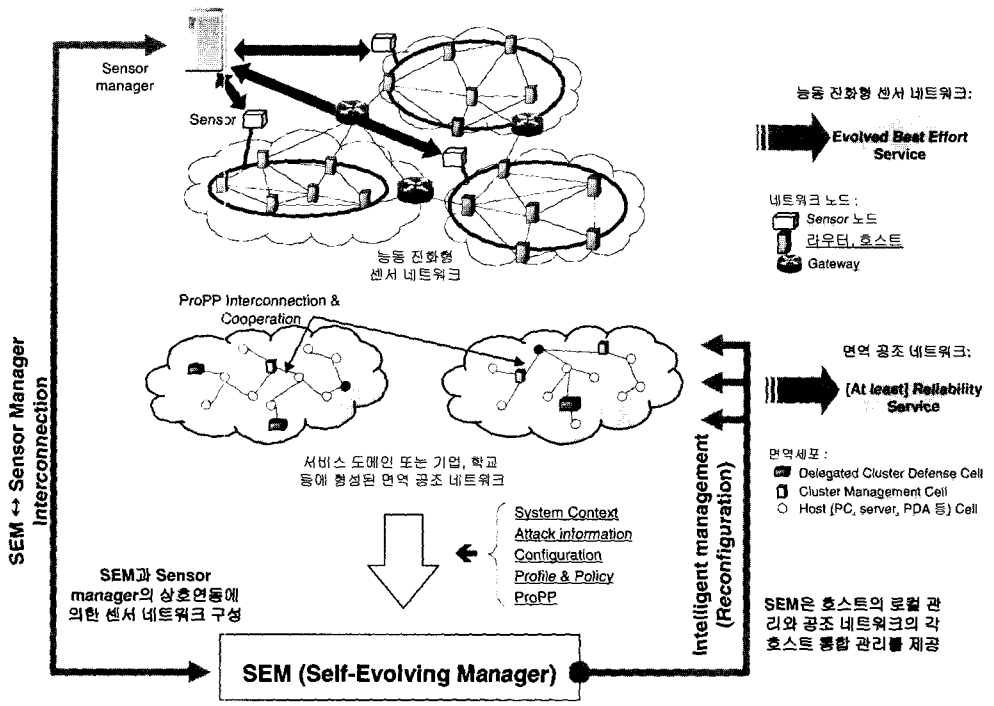

그림 3 보안 인프라 구조

표 1 현재의 보안 시스템과 면역 인프라의 대응책 비교

구 분	현재의 보안 시스템의 문제점	능동진화형 면역 네트워크에서의 대응책
유선망, 무선망 또는 유·무선 혼합망	· 독립적 시스템에 적용 · 실시간 대응 불가 · 시스템 리소스 낭비 · 네트워크 대응책 부재 · 공격방식 전파에 대한 대응 부족	· 플랫폼에 독립적인 plug-in 방식 · Reconfiguration으로 시스템 프로파일에 적합한 형태로 진화 · 네트워크에 기반한 실시간 탐지/대응 · 네트워크 상에서 분산된 관리체계 · 침해 호스트나 라우터 고립 등 네트워크 공격에 대한 대응책 · 자동화된 진화에 의한 사용자 편이성 극대화
차세대 네트워크	· Heterogeneity · 중앙 집중적 관리 부재 · Unexpected/Unknown user & resource · Invisibility/zero-configuration	

figuration), 신속한 대응이 가능하고 추가적인 공격으로부터 네트워크 전체를 안전하게 보호한다.

3.1.4 면역 관리 센서

공격을 탐지하기 위한 탐지 기법은 센서 네트워크의 확장된 개념으로 생각할 수 있다. 즉 센서가 네트워크의 상황을 모니터링 하여 이상 징후를 판단하는 것이다. 이러한 센서는 스위치나 라우터에 위치한 면역 agent가 시스템의 특성에 맞게 진화하여 구성된다. 면역 센서는 네트워크상의 공격이나 문제점을 스스로 진단하여 패킷을 생성하고 전체 네트워크에 정보를 제공한다. 또한 전달받은 패킷에 대해 센서 고유의 처리 프로시저를 수행하여 다른 노드로 전달함으로써 네트워크가 보다 유연하고 능동적으로 동작

할 수 있도록 한다.

3.2 개괄적 보안 인프라 구조

그림 3은 개괄적인 면역 인프라 구조를 나타낸 것이다. 면역 센서에 의해 생성된 센서 네트워크와 ProPP에 의한 면역 agent의 공조에 의해 생성된 면역 공조 네트워크가 SEM 브로커에 의해 관리되는 구조이다. 센서 네트워크는 스위치, 라우터 등에 탑재된 면역 agent가 동적 프로파일에 의해 네트워크의 다양한 상황을 모니터링하는 센서 망을 구축한다. 면역 공조 네트워크는 기업, 학교 등과 같은 크고 작은 지역망 내부의 다양한 호스트에 탑재된 면역 agent가 시스템의 프로파일에 따라 진화하면서 구축된다.

표 1은 네트워크 변혁의 측면에서 현재의 보안 시스템의 문제점과 본 논문에서 제안하는 면역 인프라의 차이점을 비교 설명한 것이다. 현재의 보안 시스템은 개별 시스템에 독립적으로 적용되고 있어 전체 네트워크 차원의 대응이 불가능하고, 많은 시스템 자원을 요구하는 경우가 대부분 이어서 차세대 네트워크를 구성하는 다양한 시스템에 적용하는데 문제점이 발생한다. 또한 하나의 호스트가 공격을 탐지하였다 하더라도 모든 호스트가 적절한 대응을 하지 못하는 단점이 있다. 이러한 보안 시스템의 특징과 차세대 네트워크의 이질성, 중앙 집중적 관리의 어려움, 사용자의 네트워크간 이동 등의 환경적 변화는 현재의 보안 시스템을 차세대 네트워크에 적용하는데 걸림돌이 된다. 본 논문에서 제안한 면역 네트워크는 진화하는 특성을 갖는 면역 agent를 이용하여 다양한 시스템 프로파일에 맞는 보안 시스템을 구축하고, 이를 이용한 공조 네트워크를 형성함으로써 이러한 문제점을 극복할 수 있다.

4. 결 론

차세대 네트워크 환경에서 이질적 호스트는 네트워크를 통한 다양한 공격에 노출될 것으로 예상된다. 그러나 현재 호스트나 지역망에 적용되고 있는 보안 시스템은 빠르게 변화하는 공격 방법에 효과적으로 대응하지 못한 채 수동적인 대응 방법만을 제시하고 있는 상황이다. 따라서 본 논문에서는 이러한 보안 시스템의 문제점을 해결하고 차세대 네트워크에 효율적으로 적용할 수 있는 새로운 보안 시스템 전략으로 면역 네트워크를 제안하였다. 본 논문에서 제안한 면역 네트워크는 시스템의 프로파일에 따라 다변화하는 면역 agent를 이용하여 분산 네트워크 상에서 보안 공조를 이룰 수 있는 새로운 인프라이다. 또한 면역 agent는 프로파일 설정에 따라 면역 인프라 관리를 위한 브로커로 진화하여 유연성, 확장성, 안전성 및 효율성을 가지는 보안 관리자로 동작할 수 있다. 본 논문에서는 이러한 면역 인프라의 핵심 요소인 면역 agent, 면역 인프라 관리, 동적 QoS 관리 등에 대해 논의하였다.

참고문헌

[1] David Moor, Vern Paxson, Stefan Savage, Colleen Shannon, Stuart Staniford, and Nicholas Weaver, "The Spread of the Sapphire/ Slammer Worm," Technical Report, http://www.caida.org/analysis/security/sapphire, 2003.

[2] Steve R. White, "Open Problems in Computer Virus Research," Virus Bulletin Conference, Munich Germany, Oct 22, 1998.

[3] Jabeom Gu, Sehyun Park, Jaehoon Nah, and Sungwon Sohn, "Security Clustering against DDoS in Pervasive Computing," Proceeding of the 4th International Workshop on Information Security Applications, pp. 679-686, 2003.

[4] Jabeom Gu, Dongwook Lee, Kweebo Sim, and Sehyun Park, "An Immunity-Based Security Layer against Internet Antigens," IEICE Transaction on Communication, Vol. E83-B, No.11, pp. 2570-2575, 2000.

[5] D. Dasgupta, "An Overview of Artificial immune systems and Their Applications," Springer, pp. 3-21, 1998.

[6] Anil Somayaji, Steven Hofmeyr, and Stephanie Forrest, "Principles of a Computer Immune System," Proceeding of New Security Paradigms Workshop, Langdale, Cumbria, pp. 75-82, 1997.

[7] Charles A. Janeway, Paul Travers, Mark Walport, and J. Donald Capra, "Immu

nobiology: The Immune System in Health and Disease," 4th edition, Current Biology Pub., pp. 1-30, 1999.

[8] M. Frodigh, S. Parkvall, C. Roobol, P. Johansson, and P. Larsson, "Future Generation Wireless Networks," IEEE Personal Communications, Vol. 8, No. 5, October, 2001.

[9] T. Otsu, I. Okajima, N. Umeda, and Y. Yamao, "Network Architecture for Mobile Communications Systems Beyond IMT-2000," IEEE Personal Communications, Vol.8, No. 5, October, 2001.

[10] K. W. Richardson, "UMTS overview," Electronics & Communication Engineering Journal, Vol. 12, No. 3, June, 2000.

[11] G. Patel and S. Dernett, "The 3GPP and 3GPP2 Movements Toward an All-IP Mobile Network," IEEE Personal Communications, Vol. 7, Issue 4, August, 2000.

구 자 범

2000 중앙대학교 전자전기공학부(학사)
2002 중앙대학교 전자전기공학부(석사)
2002~현재 중앙대학교 전자전기공학부 (박사과정)
관심 분야 : Pervasive computing 보안, 무선 인터넷 보안, 차세대 글로벌 면역 시스템
E mail jabeom@ms.cau.ac.kr

박 세 현

1986 중앙대학교 전자공학과(학사)
1988 중앙대학교 전자공학과(석사)
1998 컴퓨터 공학 박사, University of Massachusetts at Amherst, ECE Dept.
1988. 2~1999. 2 한국전자통신연구원, 선임 연구원
1999. 3~현재 중앙대학교 전자전기공학부 조교수
관심 분야 : 홈네트워크보안, 유비쿼터스 보안, 무선네트워크보안, 웹서비스 보안, LBS Privacy, 개인정보보호
E mail : shpark@cau.ac.kr