韓國 컴퓨터情報學會 論文誌
第11卷 第3號, 2006. 7.

2006-11-3-2-4

퍼베이시브 컴퓨팅 환경에서의 침입탐지용 모바일 에이전트에 대한 연구

오병진*, 엄남경*, 문형진*, 이상호**

Study on mobile agents for the intrusion detection in pervasive computing environment

Oh Byung-jin*, Um nam-kyoung*, Mun hyung-jin*, Lee sang-ho**

요 약

퍼베이시브 컴퓨팅 환경은 미국 표준화 기구인 NIST와 IBM이 함께 추진하고 있는 개념으로써 유비쿼터스와 유사한 의미이나, 개념적으로만 쓰이는 유비쿼터스와는 대조적으로 IBM에서 추진하는 하나의 사업적 상품명으로 취급되고 있다. 이러한 환경에 기초하여 침입탐지용 모바일 에이전트에 대한 연구가 함께 진행 중이다. 이 논문에서는 침입탐지를 위한 모바일 에이전트에 대한 연구를 다룬 후, 침입 탐지에 있어서 다중 모바일 에이전트를 기반으로 이동중의 모바일 에이전트를 이용한 침입 탐지 시나리오를 제안한다. 이를 통해 침입 탐지에 있어서 무결성 이동성의 과정에서 발생하는 침입 탐지 문제를 해결할 수 있었다.

Abstract

Pervasive computing environment is similar to the meaning of ubiquitous computing, however it is a kind of the commercial product, which is made from the collaboration between NIST and IBM. On the basis of this environment, the research of mobile agents for intrusion detection is going on in progress. In this paper, we study the research about mobile agents for the intrusion detection and then suggest scenarios using moving mobile agents based on the multiple mobile agents in the intrusion detection. Subsequently, we could figure out the problems which occurred through progress of integrity movement as a matter of the intrusion detection.

▸ Keyword : 침입탐지(Intrusion Detection),모바일 에이전트(Mobile Agent),퍼베이시브 컴퓨팅 환경 (Pervasive Computing Environment)

• 제1저자 : 오병진
• 접수일 : 2006.05.30, 심사일 : 2006.06.21, 심사완료일 : 2006.07.10
* 충북대학교 전자계산학과 박사수료 ** 충북대학교 전기전자 및 컴퓨터공학부 교수

Ⅰ. 서 론

퍼베이시브 컴퓨팅 환경에서는 컴퓨팅 기술과 커뮤니케이션의 조합이 가속화 되면서, 정보 접근의 편의를 증진시킬 수 있게 된다. 그러나 컴퓨팅과 커뮤니케이션이 대중의 일상생활에 실질적으로 적용되어서 우리 업무의 효율성을 증대시키고 삶의 질을 향상시키는 단계에 가기 위해서는 법의학이나 무결성 이동성(데이터나 트래픽 등의 무결성이 보장되는 조건 하에서 이루어지는 개체의 이동 현상)등과 같은 많은 중요한 문제들이 우선적으로 연구되어져야 한다. 특히 침입 행위란, 정보시스템의 무결성을 저해하는 일련의 행동이나 정보시스템의 보안 정책을 위반하는 행위를 말한다. 침입 행위를 탐지하기 위한 시스템을 침입 탐지 시스템이라 한다. 침입에 사용되는 데이터의 출처를 가지고 네트워크 기반 및 호스트 기반의 침입 탐지 시스템으로 분류할 수 있으며, 탐지 모델에 따라서는 그림 1과 같이 비정상행위 탐지와 오용 탐지 방식으로 나눌 수 있다. 일반적으로 호스트 기반의 침입 탐지 시스템과 같은 독점적 솔루션을 네트워크에 있는 모든 호스트에 설치하는 것은 지나치게 비싸다. 그러나 모바일 에이전트용 플랫폼이나 자바 가상 머신과 같은 일반적 목적의 인터프리터를 모든 호스트에 설치할 수도 있다. 모바일 에이전트들을 이용함으로써 정적 요소만을 채택하고 있는 기존의 침입 탐지 시스템의 제한을 극복할 수 있다[5]. 이동성과 자율성의 속성들은 실제 세계의 유사성을 따르는 탐지 설계를 이상적으로 만들 수 있다. 따라서 이러한 속성을 잘 이용하면, 침입 탐지와 같은 중요한 분야에서 필요한 지식적인 부분을 충족할 수 있을 것이라 본다.

따라서 이 논문에서는 침입 탐지에 있어서의 모바일 에이전트의 이점 및 분류와 함께 기법들을 소개할 것이다. 또한 침입을 탐지함과 동시에, 무결성 이동이 가능한 모바일 에이전트를 위한 시나리오를 제시할 것이다.

Ⅱ. 본론

1. 침입 탐지를 위한 모바일 에이전트

모바일 에이전트는 분산된 네트워크 환경에서 한 노드에서 다른 노드로 자체적으로 이동할수 있는 독립적인 프로그램의 일종이라 할 수 있다. 모바일 에이전트의 장점은 전통적인 방식인 클라이언트/서버 모델이나 요구시 코드 방식과 비교하여 볼 때, 다음과 같은 특징을 가지고 있다.

1) 네트워크 지연 극복

모바일 에이전트들은 지시에 대해서 빠른 수행과 처리를 할 수 있고, 그들의 환경을 바꿀 수 있도록 실시간 응답을 허용한다. 또한 탐색과 잠재적인 네트워크 침입을 탐지하는 것 등도 모바일 에이전트에서 제공할 수 있다.

2) 자율적, 비동기적 실행

네트워크에 널리 퍼져있는 시스템에서, 시스템의 일부가 손상되거나 격리되어도 작동을 계속할 수 있도록 하는 수행능력은 매우 중요하다. 공격으로부터 살아남은 에이전트들은 위협을 입은 요소들을 복제 등에 의해 재건하고 기능을 회복하게 할 수 있기 때문에, 모바일 에이전트들은 플랫폼을 만드는 것 뿐 아니라 침입 탐지 시스템의 한 요소로서 활용하는 것을 통해 독립적으로 작동 및 존재할 수 있도록 한다.

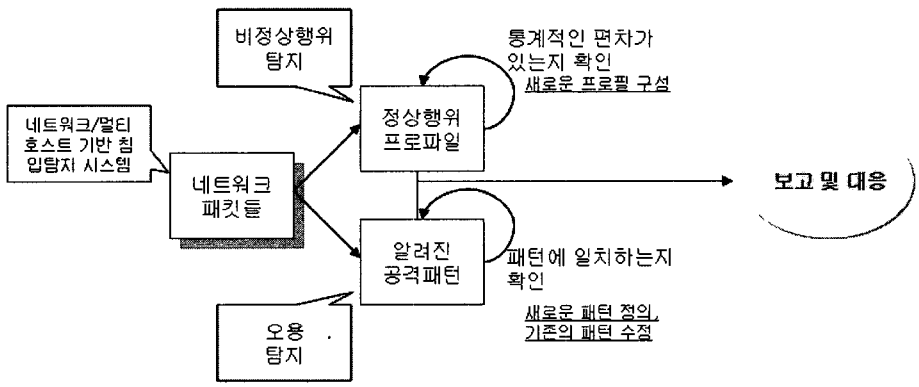

그림 1. 침입 탐지 시스템의 침입 분석 방법
Fig 1. Intrusion analysis method of intrusion detection system

3) 동적 적응

침입 탐지에 있어 모바일 에이전트 시스템이 그들 스스로 환경을 감지하고 변화에 반응하는 능력은 매우 중요한 것이다. 특히, 에이전트들은 활동하기에 보다 나은 위치로 이동하거나, 위험을 피하고, 스스로를 복제하거나 또는 보조를 맞추기 위해, 또한 다른 에이전트들을 정렬시키기 위해 어디로든 움직일 수 있다. 에이전트들은 또한 유리한 상황으로 조정할 수 있다. 즉, 자율성과 비동기성의 실행이 복합되었을 때, 이러한 특성은 강력하고 실패를 견딜 수 있는 시스템 등의 구축을 용이하게 한다.

또한 모바일 에이전트는 그림 2와 같은 여러 단계의 라이프 사이클을 가지고 있다. 각 단계들은 생성, 중지, 실행, 서비스 탐색, 새로운 호스트에 도착, 이동, 원래의 호스트로 귀환, 종료 등으로 구성되어 있으며, 크게 자원들, 보조정보, 메소드 등의 세 부분으로 나누어져 있다.

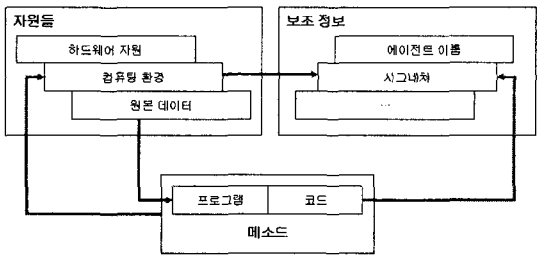

그림 2. 모바일 에이전트의 구성
Fig 2. Component of mobile agent

2. 모바일 에이전트의 분류 및 기법

모바일 에이전트는 본래 자율적이고, 협력적이고, 자가구성을 하며, 이동성을 갖고 있다[6]. 이러한 기능들은 전통적인 배포된 프로그램에서는 찾을 수 없는 것으로써, 침입 탐지 시스템에게 완전히 새로운 접근 방법을 시도할 수 있도록 하고, 일부는 자연과 사회에서 발견한 공통점에 바탕을 두고 있는 것도 있다. [5]와 같은 다른 연구에서나 침입 탐지 전략에 있어 차이점이 있기 때문에, 이 장에서는 모바일 에이전트의 분류와 그에 대한 실행 기법 들에 대해 소개한다. 무결성 전송에 있어서, 침입은 불법접근, 모든 종류의 유효하지 않은 채널 또는 접근 등을 통한 적의가 있는 공격 등을 포함한다. 따라서 탐지 기법으로는 모니터링, 감사(Auditing), 분석, 경고, 응답 등을 포함한다.

2.1 무결성 전송을 위한 모바일 에이전트 분류

모바일 에이전트의 기능을 기준으로 다음과 같이 세 가지로 분류할 수 있다[4].

- **터미널 에이전트**
  TA(Terminal Agent)로써, User Agent(UA)를 포함
- **네비게이션 에이전트**
  VA(naVigation Agent)로써, 네트워크 용량 에이전트(Network Capability Agent: NCA), 침입 탐지 에이전트(Intrusion Detection Agent: IDA) 그리고 Location Management Agent(LMA)를 포함
- **태스크 에이전트**
  TA(Task Agent)로써, 실행코드 에이전트(Execution code Agent: EA), 서비스 에이전트(Service Agent: SA)와 같은 데이터 에이전트(Data Agent: DA), 사용자 문서 데이터베이스 에이전트(User Document Database Agent: UDDA)를 포함

모바일 에이전트는 능동적으로 언제 어디로 전송할 것인지를 결정하는 작업이 가능하므로, 어떤 시점이나 다른 컴퓨터로 전송되는 작업을 멈추게 할 수 있으며, 이러한 작업을 연속적으로 실행할 수 도 있다. 이것은 또한 인터넷과 같은 광범위한 다중의 네트워크 환경에도 적합하다.

[1]의 연구에서 모바일 에이전트 시스템(Mobile Agent System: MAS)은 생성, 설명, 실행, 예약, 전송 그리고 종료 에이전트를 위한 일종의 플랫폼이다. 각 시스템은 많은 에이전트를 운영할 수 있다. 만약 전송된 데이터가 부분적이고, 이 부분의 정보는 반드시 먼저 전송되어야 한다면 그 작업이 복구할 수 있기 위하여 런타임 환경을 목적 노드(target node)에서 연속적으로 운영하기 위해, 이 부분의 실행코드, 운영 상태등과 같은 정보는 키셋(Key set)으로 간주할 수 있다. 위에서 언급한 에이전트들의 분류에 기반으로 아래와 같은 규칙이 적용될 수 있다.

모바일 에이전트를 위한 규칙(rule of mobile agent)

네비게이션 에이전트는 위상적 구조 네트워크에서의 목적노드와 어드레싱(addressing)의 서브넷의 위상적 구조에 가까운 작업에 대해서 직접적으로 관계된 일을 할 필요가 없다.
태스크 에이전트는 코드 실행, 데이터 및 환경 상태 관리 등과 같은 것을 포함하는 세부적인 일을 한다. 그것은 네트워크에 있는 네비게이션 에이전트에 전송할 수 있으며 서브넷의 구조를 알 필요가 없다.
태스크 에이전트는 전송시에 관련된 네비게이션 에이전트를 찾는다. 그 후에 데이터베이스를 찾고, 네비게이션 에이전트에 의해 목적노드를 보낸다. 이와 함께 새로운 공격을 탐지할 수 있게 된다.

2.2 무결성 전송을 위한 다중지점 탐지기법

침입 탐지 수집 요소를 쉽게 재설정하고, 가벼운 소프

트웨어 요소의 집합을 구조화하기 위해서 주로 사용되어지는 방식은 전통적인 침입 탐지 시스템에서의 기법이라 할 수 있다. 각 에이전트들은 무작위로 네트워크를 운행하면서 일(task)들을 수행하는 것이 가능하다. 운행 중에 침입의 가능성을 가진다면, 에이전트는 사이트에 대한 추가적인 실험을 제시하거나 요구할 수 있다. 또한 최종적으로 침입에 대한 의심적인 레벨(level)이 높아지면, 실질적으로 경고(alarm) 또는 알림(notice)을 보낼 수 있을 것이다. 공격시에는 공격과 관련된 실험을 통해 목적 노드에 알림 정보를 주는 것에 주의한다. 그리고 각 실험들은 모든 노드에 상주해서 남아있을 필요가 없다. 무작위 샘플링은 오랜 기간동안 제조업에서 품질 제어를 위해 성공적으로 사용되어 왔다. 근본적으로, 만약 랜덤 샘플링에 의해 문제가 포착되면, 좀 더 포괄적으로 일련의 실험을 함으로써 문제에 대해 해결하도록 실행되어져야 한다. 이동하는 모바일 에이전트 탐지기들은 정적으로 설치된 예외 탐지기에 접속할 수 없기 전에 이벤트를 생성할 수 있다. 에이전트들은 네트워크 또는 호스트들의 성능에 대한 통계를 모으는데, 이것은 개별 노드에서는 의미를 갖기 어려우나 각각의 자료가 모아지면 의미를 가질 수 있다. 전체 네트워크를 포함하여 각각의 이벤트들을 연관시킴으로서, 낮은 탐지 오류율로 새로운 공격을 탐지하는 것이 가능하다.

침입탐지 시스템은 분산되었거나 단계적으로 발생하는 공격들을 탐지해내기 위해 여러 장소에서의 이벤트들을 분석함으로서 다중지점 탐색을 수행한다. 이 이벤트들은 여러 호스트, 어플리케이션 또는 네트워크 인터페이스로부터 올 수 있다. 다중지점 탐지는 침입탐지시스템이 모든 분산된 이벤트들을 처리할 수 있음에도 불구하고 기술적으로 해결하기 어려우나, 일부 침입탐지 시스템들은 분산된 이벤트들의 처리를 위해, 일반적으로 대량의 로그(log)를 중앙으로 집중된 위치로 움직이기 위한 네트워크 대역폭상의 여유를 제공할 수 있다. 침입탐지 시스템은 침입탐지 시스템 제조업자(vendor)들이 사용하는 보편적인 해결책을 통해 이벤트들을 통합하기 전에 각각 분산된 로그 파일에서 필터링과 데이터 요약을 수행하는 것이다. 그러나 현재 요약된 자료를 쓰고 있기 때문에, 이것은 분산되어 있는 공격들을 잡아내는 데에 어려움만을 더하게 된다.

호스트에서의 공격과는 반대로 무결성 이동성 네트워크에서 공격을 포착하기 위해 다중지점 탐지는 매우 유용하게 된다. 이는 집단 공격의 목표가 부분적인 호스트가 아니라, 네트워크 자원에의 접근을 얻어내는 것일 수 있다.

모바일 에이전트들은 게이트웨이에서, 호스트들에서, 서버들에서 그리고 다른 외부에 노출된 포인트에서부터의 공격을 관련시킴으로서 이 전략을 적용할 수 있다:

2.3 구조에 대한 공격 기법

침입탐지 시스템들은 효율성과 중앙 집중 제어를 위해 계층적 구조를 사용하게 된다. 핵심 요소들의 실패를 보완하기 위해 관계를 능동적으로 재설정할 수 없는 계층적 구조의 침입탐지 시스템을 가정해 보자. 단일 지점 탐지는 각 리프노드(leaf node)에서 일어난다. 리프노드들로부터의 결과는 데이터 요약을 수행하며 다중 지점 탐지를 하고 있는 내부 노드 계층의 상부로 보내진다. 데이터는 루트(root)의 명령 및 제어 노드에 도달할 때까지 계속해서 요약된다. 이렇게 설계된 구조는 실패한 다른 많은 단일 지점들의 결과로부터 중복 통신라인을 갖고 있지 않으므로, 공격자는 침입탐지 시스템의 내부 노드를 공격함으로서 제어 분기를 절단하거나, 루트를 끌어냄으로서 침입탐지 시스템을 무력화시킬 수 있다. 모바일 에이전트를 이용한 표준의 계층적 침입탐지 시스템들은 각각의 노드를 백업하고, 공격자의 시야 밖에서 잃어버린 기능을 복구한다. 공격 행위가 발견되면 모바일 에이전트 침입탐지 시스템들을 재배치한다.

2.4 자동화된 응답 기법

무결성 이동성 하에서, 침입탐지 시스템이 작동하는 네트워크 안에서 공격자들의 경로를 추적하는 침입탐지 시슬템을 가정해보자.

이 기능이 유용한 이유는 다음의 두가지와 같다. 첫째, 공격자들은 목표를 공격하기 전에 종종 많은 호스트들의 연결을 통해 로그를 남긴다. 따라서 이 연결을 통해 뒤를 쫓아 공격자의 로그를 찾아내야 한다. 둘째, 공격자들은 종종 그들의 발신 주소를 속일 수도 있다. 이 패킷들의 실질적인 출처를 찾아내야 한다. 때문에 패킷들을 원본 랜(LAN)을 찾을 때 까지 랜에서 랜으로 추적하는 방법이 필요하다. 패킷을 보내는 실제 호스트를 찾기 위해서는 랜 안에서 직접 호스트를 방문할 필요가 있다. 공격자들은 IP 주소를 속이는 것만큼, 맥(MAC) 주소까지 속일 수 있기 때문이다. 대부분의 공격들은 네트워크의 외부에서 오기 때문에 완전히 끝까지 추적할 수 없다. 그러나 내부 공격은 공격이 내부에서 오든, 외부에서 오든 침입탐지 시스템 자체에서 어디에서 오는지를 결정해야 하며, 가능한 한 공격자의 위치를 찾아낼 필요가 있다: 실제적으로 랜에서 랜으로의 공격에 대한 공격자를 찾기 위해서는 모든 네트워크 내의 이더넷 구역들을 스니핑(sniffing) 할 수 있어야 한다. 자신의 신원을 속인 이더넷 구역에서 호스트를 찾기 위해서는 각각의 이더

넷 구역 위에 있는 호스트들을 분석해야 한다. 따라서, 네트워크 침입탐지 시스템을 통해 공격자를 충분히 추적하기 위해서는 모든 이더넷 구역을 스티핑하고 모든 호스트를 분석할 수 있어야 한다. 보통 인프라 구조에서 이런 종류의 추적을 지원하기 위해서는 상당한 비용이 소요된다. 따라서 추적 시스템이 다루어야 할 몇가지 문제들은 다음과 같다. 만약 공격자가 호스트와 타협되었다면 모바일 에이전트 플랫폼은 아마도 제 기능을 하지 못할 것이다. 따라서, 모든 추적 시스템들은 많은 위치로부터 결과를 비교해서 데이터를 모아야 할 것이다. 최종적으로, 공격자가 그의 공격 연결 내의 각각의 링크를 통해 보내는 것은 완전히 다른 데이터 일 것이다. 한 예로, 공격자는 링크 암호화를 사용할 수도 있다: 이 시나리오 안에서, 공격자를 추적하기 위해 시스템은 매우 정교한 인공지능 기술 또는 결정을 내릴 수 있는 알고리즘을 필요로 할 것이다. 모바일 에이전트 플랫폼의 존재를 가정하면, 추적 시스템은 전 네트워크에 쉽고 빠르게 자동적으로 배치될 수 있을 것이다.

III. 실험

연구 [9][10]의 시험작 시스템의 하나인 MA들에 의해 지원되는 스마트 클래스 룸은 Pervasive 컴퓨팅으로부터 고무되었다. 임베디드 컴퓨터들, 정보 어플라이언스들, 그리고 멀티모달 센서들로 구성된 작업 환경은 사람들에게 전례없는 수준의 정보에의 접근 및 컴퓨터로부터의 도움을 제공함으로서 사람들에게 효율적으로 작업을 수행할 수 있도록 해 줍니다.

1. 침입탐지 에이전트 시험

침입탐지 에이전트 시스템은 침입탐지 시스템에 기반한 다중의 호스트이다[8]. 사용자의 행동을 분석하는 대신, 침입탐지 에이전트는 침입과 관련된 특정한 이벤트들을 주시함으로서 효과를 발휘하는데, 이러한 이벤트들을 의심되는 침입자의 흔적(Marks Left by Suspected Intruder, MLSI)라고 한다. 만약 MLSI 가 발견되면, 침입탐지 에이전트는 해당 MLSI 에 관련된 정보를 모으고, 분석하여 침입이 일어난 것인지 아닌지 결정한다. 침입탐지 에이전트 시스템은 침입과 관계된 다양한 호스트 속에서 침입자를 추적하고, 정보를 모으는 데에 있어 모바일 에이전트에 의지한다.

이 구조는 루트에 중앙 관리자와 리프노드들의 다양한 에이전트로 구성된 계층적 구조를 갖고 있다. 침입 정보를 발견하면, 센서는 급히 호스트의 에이전트를 추적하고 있는 관리자에게 알린다. 근원지로 의심되는 식별된 다른 위치로 이동하기 전에 호스트에서 관련된 정보를 모으기 위한 정보 수집 에이전트를 시작한다. 관리자는 그들이 리턴 되는대로 정보 수집 에이전트로부터 결과를 모아서 종합한다. 이 논문에서 제시하는 침입 탐지 프레임워크는 기능과 요소들을 이해하고 논의하는데 유용한 관점을 제시한다. 침입탐지 프레임워크에서 각 요소들은 다음과 같다.

1) 데이터 감사 유닛(Data Audit Unit)
감사 자료 필터, 강도 경보기 또는 다른 계산적 환경으로부터의 이벤트를 얻기 위한 센서들이 해당된다.

2) 분석기(Analyzer)
이벤트 필터, 공격 징후 탐지기, 종합적 이벤트 프로 파일러와 같은 다른 요소로부터의 침임탐지 정보를 분석하고 새로운 침입탐지 정보를 리턴하기 위한 요소이다. 침입 탐지 정보는 시스템에서 일어난 이벤트와 그 분석정보, 이행되어야 할 규칙 또는 이벤트에 대한 처리 요구를 포함한다.

3) 응답 유닛(Response Unit)
다른 요소들로부터의 지시를 수행하는 요소를 뜻하며, 지시는 프로세스를 제거하거나, 접속을 재설정하거나, 다른 요소들을 위한 응답 유닛을 만드는 등의 요청이다.

4) 연결 유닛(Matchmaker Unit)
다른 요소들과 연결하는 설정 및 디렉토리 서비스를 제공하는 요소로써 연결기는 이름이나 서비스로 협동 요소들을 지정하도록 해준다. 이것은 계층적, 네트워크 또는 하이브리드 구조로 구성될 수 있다. 이것은 또한 푸쉬(push), 풀(pull) 형태의 인터페이스를 지원할 수 있다. 형성자는 요소에 의한 침입탐지 정보의 자발적인 생성을 지시하고 후에는 생성된 침입탐지 정보를 요청의 응답으로 돌려보낸다. 하나 또는 그 이상의 요소들은 같은 노드에서 합쳐지고 나란히 배치될 수 있다. 정의된 각 요소들의 대표적 형태들은 침입탐지 시스템의 주요기능들이다.

2 모바일 에이전트의 이용 시험

전송된 작업의 내용의 완전함에 따라, 작업의 모바일 입상은 "강한 전송"(또는 전체 전송)과 "약한 전송"(또는 부분 전송)으로 나누어 질 수 있는데, 전송 모드는 무작위의 명령 또는 이동 계획일 수 있다. 강한 전송이란 목적 터미널에 도달한 뒤 현재 작업과 관련된 전체 정보가 전송되는 것

을 뜻하며, 작업은 단편적 위치로부터 연속적으로 실행될 수 있다: 그러나 모바일웹에 있어서, 실행 상태를 설명하고 기록하기 위한 현재 작업의 모든 정보를 얻는 것은 어렵고, 고대역(high broadband) 네트워크에서의 작업을 필요로 하기 때문에 이러한 부류의 모드는 매우 무겁고 복잡하다. 일반적으로, 약한 전송은 부분적인 실행 상태와 데이터만 이루어지며 강한 전송에 비해 훨씬 빠르고 지연시간도 매우 짧습니다. 약한 전송하에서, 특정MAS는 Aglet, Mole 등과 같은 무작위 명령을 채택한다. 대신 약한 전송은 작업의 전체 구조적 실행 상황은 복구되기 어려우며, 설계와 디자인이 어렵다는 결점을 갖고 있다. 따라서 적용에 있어서 어떤 모드를 채택할 것인지는 자세한 시나리오에 따라서만 결정된다. 다른 유사한 스마트 스페이스/지능적 주변 환경 설치와 같은 다중 모바일 에이전트들에 의한 스마트 클래스룸은 적절한 수의 프로젝터, 카메라, 센서, 얼굴 인식, 음성 인식, 안구 인식 모듈등과 같은 하드웨어와 소프트웨어 모듈을 모을 것이다. 제한된 계산 능력과, 엄청난 관리 요구점들로 인해 이 모든 요소들을 한대의 컴퓨터에 설치하는 것은 상상조차 할 수 없다. 따라서, 지능적 주변 환경 구성에 있어 분산 컴퓨팅 구조가 필요하다. 이 논문에서 제시하는 침입탐지 시스템 요소를 위해 모바일 에이전트를 이용함으로써 얻는 몇가지 특징은 다음과 같다.

1) 네트워크 트래픽 탐지기 (Network Traffic Detectors)
네트워크 트래픽의 지속적인 증가를 버텨내는 것은 커널이나 특별한 목적의 하드웨어의 일이 될 것으로 보인다. 모바일 네트워크 트래픽 모니터는, 만약 그것이 지금까지 네트워크 트래픽을 견딜 수 있다면, 불법적 침입에 의해 다른 장비로 옮겨질 때 정보를 잃게 될 것이다. 모바일 에이전트는 네트워크 트래픽을 직접 감시하기에는 적절치 않으며, 다만 네트워크 센서에서 데이터 분석기로부터 제공된 자료만을 감시한다.

2) 호스트 기반 분석기(Host-Based Analyzer)
모바일 에이전트들은 유선망에서는 불가능한 정보들을 모으기 위해 워크스테이션, 방화벽, 라우터 등과 같은 호스트에 갈 수 있다. 분석 에이전트들은 감사 로그를 처리하고, 분산된 네트워크 트래픽 모니터들로부터의 데이터를 연관시키며 네트워크 모니터들로부터 얻어진 정보를 처리한다. 새로운 공격이나 새로운 패턴의 의심스러운 행동이 발견되면, 다른 것들은 더 이상 쓸모가 없기 때문에 분석기는 업그레이드 되어야만 한다. 분석 에이전트들은 데이터가 존재하는 호스트 플랫폼에서는 지원되지 않는 특화된 데이터 검색을 수행할 수 있다: 이 에이전트들은 네트워크를 다시 설정하기 위해 네트워크 내를 돌아다닐 수 있으며, 이것은 결정을 내리거나 관리 작업을 수행하지 않는 가벼운 클라이언트들에게 있어 특히 유용한다.

3) 조정기(Coordinators)
협조적 방식으로 문제를 분해, 해결할 수 있는 에이전트들은 무결성 전송 하에서의 적대적 공격들을 탐지하기 위한 많은 수의 도메인들을 위한 지능 에이전트 공동체에 의해 성공적으로 개발되었습니다. 침입 탐지 에이전트는 관찰하고, 판단하며, 다른 침입탐지 에이전트들과 상호 작용하고, 다른 모바일 에이전트들과 함께 동시 행동을 수행한다. 상호작용은 일반적 이해를 위해서는 형이상학에 의존할 수 있는 에이전트 의사소통 언어를 통해 사실이나 믿음관계를 전달할 수 있다. 다른 IDS 요소도 설계하였지만, 이는 [5], [6]와 유사하다.

IV. 결론 및 향후 과제

이 논문에서는 퍼베이시브 컴퓨팅 환경 하에서 지원되는 기술에 대해 논의하였다. 또한 무결성 전송하에서의 침입탐지를 위한 다중 모바일 에이전트에 의해 얻을 수 있는 이점 등을 제시하였다. 그와 더불어 무결성을 보장하는 이동 환경에서 전송 중에 침입 탐지에 있어서 다중 모바일 에이전트를 기반으로 이동중의 모바일 에이전트를 이용한 침입 탐지 시나리오를 제안한다. 이를 통해 침입 탐지에 있어서 무결성 이동성의 과정에서 발생하는 침입 탐지 문제를 해결할 수 있었다.

우리가 제시한 기술들을 종합하여 시험 시스템에서 연구결과의 효율성에 대해 실험을 하였으나, 일부 분야에서의 성과이므로 앞으로 향후 연구에서는 전체 시스템에 대한 효율성과 성능 평가를 하도록 진행할 것이다.

참고논문

[1] 침입방지시스템 분석, ETRI 기술문서 2003
[2] Intrusion Detection, Macmillan Technical Publishing, 2000
[3] Satyanarayanan M. Pervasive Computing: Vision and Challenges[J]. IEEE Personal Communications, August 2001, 10-17.

[4] Karnik N M. Design Issues in Mobile Agent Programming Systems. IEEE Concurrency, 1999, 6,3:125.
[5] David Kotz, Robert S. Gray, Mobile Agent for intrusion detection and the Future of the Internet[J], ACM Operating Systems Review, 2002, 33(3): 7 - 13.
[6] Milojicic D. Mobile Agent applications in intrusion detection [J]. IEEE Concurrency, July-Sept, 2002, 7(3): 80- 90.
[7] Simmons R, Apfelbaum D. A Task Description Language for Robot Control[C]. Proceedings Conferece on Intelligent Robotics and Systems, New York, October 2001, 138-147.
[8] Ciancarini P. Coordinating Multi-Agent Applications on the WWW: A Reference Architecture. IEEE Trans. on Software Engineering, 2002,24(5): 363-375.
[9] Weikai Xie, Yuanchun Shi and Guanyou Xu. Smart Classroom - an Intelligent Environment for Tele-education. In Proceedings of The Second Pacific-Rim Conference on Multimedia (PCM 2001),662-668, Beijing, China. Springer LNCS2195.
[10] Yuanchun Shi, Weikai Xie, Guangyou Xu. The Smart Classroom: Merging Technologies for Seamless Tele-Education, IEEE Pervasive Computing Magazine, April-June 2003, Vol. 2, No. 2.

저 자 소 개

오 병 진(Oh Byung-jin)

1986년2월 단국대학교 전자공학과 졸업
2002년2월 한국기술교육대학교 정보통신학과 석사
2005년8월 충북대학교 전자계산학과 박사수료

〈관심분야〉 유비쿼터스 네트워크, 네트워크 보안, 침입탐지 시스템, 프로토콜 테스팅

엄 남 경

1999년2월 충북대학교 컴퓨터과학과 졸업
2002년2월 충북대학교 전자계산학과 석사
2004년2월 충북대학교 전자계산학과 박사수료

〈관심분야〉 유비쿼터스 네트워크, 네트워크 보안, 침입탐지 시스템, 프로토콜 테스팅

문 형 진

1996년2월 충남대학교 수학과 졸업
2002년2월 충남대학교 수학과 석사
2005년8월 충북대학교 전자계산학과 박사수료

〈관심분야〉 암호학, 정보보호, 컴퓨터네트워크, 네트워크보안

이 상 호

1976년2월 숭실대학교 전자계산학과 졸업
1981년2월 숭실대학교 전자계산학과 석사
1989년2월 숭실대학교 전자계산학과 박사
1981년6월~현재: 충북대학교 전기전자 및 컴퓨터공학부 교수

〈관심분야〉 통신 프로토콜 공학, 네트워크 관리, 네트워크 보안