이동 에이전트를 이용한 바이러스 탐지 시스템의 설계 및 구현

박 선영　박 승수
이화여자대학교 컴퓨터학과

Design and Implementation of a Virus Detection System using Mobile Agent

Sun Young Park,　Seung Soo Park
Dept. of Computer Science and Engineering, Ewha Womans University

요 약

최근 네트워크 기술의 발달로 컴퓨터 바이러스의 종류가 급속도로 증가하고 있음은 물론, 그 확산이 빨라지고 있으며 감염 경로 또한 매우 다양해졌다. 따라서 그만큼 자주 갱신되는 백신을 사용자들이 매번 재설치 해야하는 번거로움이 있다. 또한 현재의 치료 방법은 하나의 바이러스를 치료하기 위해 모든 바이러스를 치료할 수 있는 백신을 실행시켜야 한다. 이동에이전트는 한 기계에서 다른 기계로 이동할 수 있는 프로그램으로 때와 장소를 선택하여 이동할 수 있고 원하는 시간에 실행하거나 프로그램 자체를 또 다른 기계로 옮겨서 실행토록 할 수도 있다. 이러한 이동 에이전트 패러다임과 지능형 에이전트를 이용하여 위의 문제점을 해결할 수 있으리라고 보여진다.

1. 서 론

단순히 플로피 디스켓에 의해서 컴퓨터 바이러스가 확산되던 시대는 갔다. 이제는 광범위한 네트워크 환경의 확산으로 말미암아, 사용자가 미처 눈치채지 못하는 순간에도 바이러스는 어느 곳에나 빠른 속도로 확산되고 있으며, 컴퓨터 바이러스의 감염 경로 또한 기존의 불법 복사, 컴퓨터의 공동사용 뿐만이 아니라 네트웍을 통한 파일 공유, 컴퓨터 통신 및 인터넷을 통한 파일 전송과 전자우편, 감염된 CD-ROM 등 매우 복잡해지고 있다. 따라서 기존의 방식으로는 이러한 문제점을 완벽히 해결하기가 어려운 상황이다. [1]

소프트웨어 에이전트란 사용자를 대신하여 작업을 대행해 주는 프로그램으로 에이전트는 사용자의 지시 없이 스스로 판단하고 계획을 세우며 학습하기도 하는 능동적인 객체이다. 본 논문에서는 최근에 등장한 이동 에이전트 패러다임을 적용하여 컴퓨터 바이러스 탐지 시스템(VDMA: Virus Detection Mobile Agent)을 효율적으로 구현할 수 있는 개발환경을 시범적으로 설계, 구현하여 네트워크 기반에서 적절히 사용할 수 있는 새로운 모델을 제시해보고자 하였다.

* 본 논문은 과학기술처가 지원하는 소프트과학 기술 개발 사업 (98-NT-01-01-A-12)의 일환으로 수행되었음

2. VDMA의 설계

2.1 이동 에이전트

이동 에이전트는 네트워크상의 한 시스템에서 다른 시스템으로 자신을 전송할 수 있다. 기존의 메시지 전달 방식과는 달리 직접 작업을 수행할 수 있는 소프트웨어 객체를 전달하는 방식을 이용한 것이다. 즉 원격 프로시저 호출과 같은 방법에서처럼 지속적으로 많은 데이터를 주

고 받는 것이 아니라 프로그램 객체를 직접 이동시키기 때문에 성능이 그다지 좋지 않은 네트워크에서도 비용이나 자원을 보다 효율적으로 활용할 수 있다. [5][6]

또한 이동에이전트는 컴퓨터 사이의 대화를 패키지화하며 그것을 도착호스트에 전달함으로써 상호작용이 지역적으로 수행되도록 한다. 자신을 실행시킨 프로세스와는 독립적으로 활동하며, 비동기적으로 그리고 자발적으로 활동한다. 이동에이전트는 실행환경에 반응하고, 그 변화에 자발적으로 대응하는 능력을 가지고 있다. 다수의 이동에이전트는 네트워크의 호스트사이에 자신을 분산시킬 수 있으며, 따라서 특정 문제를 해결하기 위한 최적의 설정을 유지한다. 이동에이전트는 일반적으로 컴퓨터/전송계층 독립적이고 그 실행환경에만 종속적이기 때문에 지속적인 시스템 통합을 위한 환경을 제공해준다. [2]

2.2 전체 시스템 구성

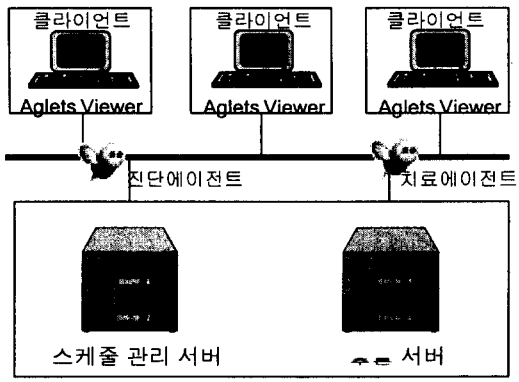

그림 1 VDMA의 전체적인 구성

VDMA는 그림 1과 같이 이동 에이전트들이 클라이언트로 가는 주기와 클라이언트의 제반사항에 따른 계획을 세워주는 스케줄 관리서버와 바이러스를 발견했을 때 적절한 백신을 추론해주는 추론서버가 있으며, 이동 에이전트는 스케줄 관리 서버의 지시에 따라 클라이언트가 바이러스에 감염되었는지 체크하는 진단 에이전트와 추론서버의 결과에 따라 백신을 가져가서 바이러스를 없애는 치료 에이전트로 구성된다.

3. VDMA의 구현

VDMA의 구현을 위해 시스템은 PC를 사용하였으며 운영체제는 Windows 95/98, Windows NT에서 모두 동작한다. 자바 개발 도구인 JDK 1.1.7, 이동 에이전트 시스템 개발 도구인 Aglet Workbench, 그리고 전문가 시스템 개발도구인 Jess5.0a5를 사용하였다.

3.1 사용자 인터페이스

VDMA는 이동 에이전트 서버를 이용하여 생성되는 Aglet으로 구현된 사용자 인터페이스를 가지고 있다.

3.2 ATP의 개요

ATP(Agent Transfer Protocol)는 분산 에이전트 기반 시스템들을 위한 응용 계층 프로토콜이다. 이것은 네트워크에 연결된 컴퓨터들 사이에서 이동 에이전트들의 이동을 위해 사용될 수 있다. 이동 에이전트들은 서로 다른 언어로 가상 기계를 포함한 여러 가지 에이전트 플랫폼 위에서 프로그램 될 수 있다. ATP는 에이전트들의 이동성을 일반적인 정형화된 방법으로 다룰 수 있는 기회를 제공한다. ATP는 IBM Aglet Workbench의 일환으로 개발되었으며 현재 버전 1.1.b1을 인터넷을 통해 다운 받을 수 있다.

에이전트는 사용자의 편의를 위한 작동들을 하는 프로그램이며 사용자가 추구하는 목표를 만족시키기 위해 어느 정도의 자율성을 갖는다. 이동 에이전트는 네트워크를 통해 이동할 수 있는 능력이 있다. 자신의 실행을 중단시키고 자신의 상태를 유지하면서 네트워크상의 또 다른 호스트로 이동하여 이동된 목적 호스트에서 재실행될 수 있다. ATP는 인터넷상에서 네트워크에 연결된 컴퓨터들 사이를 에이전트들이 이동하기 위한 간단하고 플랫폼에 독립적인 프로토콜이다.

3.3 구현 예

구현된 시스템에서 입력되는 정보는 클라이언트의 리스트와 간단한 사용자 프로파일이다. 스케줄 에이전트는 클라이언트로 진단 에이전트를 보내는 주기와 사용자 프로파일에 따른 계획을 세운다. 진단 에이전트는 클라이언트로 가서 바이러스에 감염되었는지 체크한 후 되돌아와 그 결과를 추론 에이전트에게 준다. 추론 에이전트는 증상에 따른 알맞은 바이러스 백신을 결정하고 감염된 클라이언트에게 치료 에이전트를 보낸다. 치료된 결과는 스케줄 에이전트에 다시 적용되며, 이후에 스케줄 에이전트의 계획에 반영된다.

VDMA의 전체적인 흐름은 그림 2와 같다.

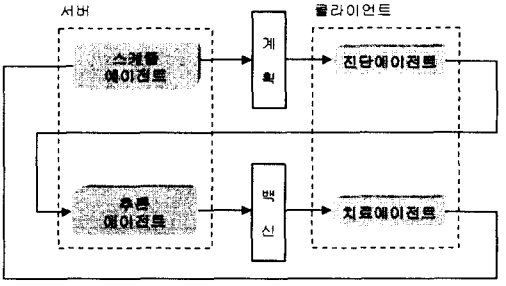

그림 2 VDMA의 전체적인 흐름

3.4 시스템의 동작 시나리오

동작 시나리오는 다음과 같다.

I. 서버의 스케줄 에이전트가 세운 계획에 따라 주기적으로, 그리고 바이러스가 활동하는 특정일에 맞추어서 네트워크상의 클라이언트들에게 진단 에이전트를 보낸다. 진단 에이전트는 서버로 되돌아올 때 바이러스가 있으면 그 결과를 추론 에이전트에게 전달한다.

II. 서버의 추론 에이전트는 진단 에이전트의 결과에 따라 적절한 백신을 추론한다. 이때 추론 에이전트는 어떤 바이러스에 감염되었는지 추론을 한 후, 그 바이러스를 치료할 수 있는 백신을 선택하여 치료 에이전트에게 보낸다.

III. 치료 에이전트는 바이러스에 감염된 각 클라이언트로 이동한 후 치료가 완전히 끝날 때까지 상주한다.

IV. 치료 에이전트는 치료가 끝나면 서버로 되돌아와서 수행결과를 저장하고, 그 결과는 이후 스케줄 에이전트와 추론 에이전트의 계획에 지속적으로 반영된다.

VDMA의 수행결과는 다음과 같다.

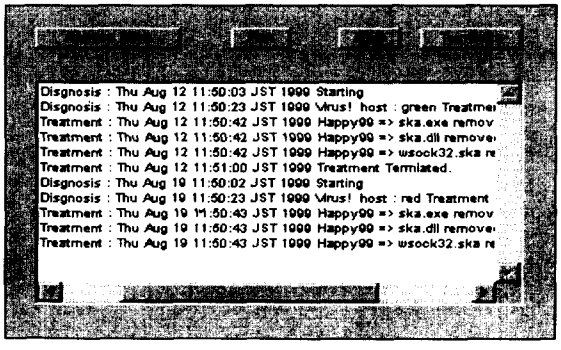

그림 3 VDMA의 수행결과

4. 결 론

이동에이전트란 네트워크를 돌아다니며 수행되는 에이전트로 클라이언트의 요구에 의해서가 아니라 자신의 판단에 의해 움직인다.

최근 네트워크 환경의 발달로 컴퓨터 바이러스의 확산이 빨라졌고, 그에 따른 백신의 갱신도 자주 일어나고 있는데 이는 사용자들이 매번 다운로드 해야하는 불편함이 있을 뿐 아니라, 사용자가 자주 백신프로그램을 실행시켜야하는 번거로움이 있다.

VDMA가 갖는 기대효과 및 의의는 다음과 같다.

- 항상 최신의 백신으로 인트라넷 환경 전체의 바이러스를 검색하고 치료할 수 있다.
- 에이전트를 이용하여 사용자들의 불편을 최소화하고 효율성과 실효성을 극대화한다.
- 바이러스에 무지한 사용자에 의해 다른 시스템까지 바이러스에 전염되는 것을 막을 수 있다.
- 사용자가 모두 백신 프로그램을 가지고 있지 않아도 된다.

5. 참고문헌

[1] 안철수, "바이러스 분석과 백신 제작", 정보시대, 1994

[2] "Mobile Agent Facility Specification", Joint Submission : Crystaliz, Inc., General Magic, Inc., GMD FOKUS, International Business Machines Corporation, OMG TC Document cf/xx-x-xx, June 2, 1997

[3] "Mobile Agents: Are they a good idea?" , IBM Research Report

[4] Lange, D. B., Mitsuru Oshima, "Programming and Deploying JAVA Mobile Agents with Aglets", Addison Wesley, 1998

[5] Nwana H., "Software agents: An Overview", Knowledge and Engineering Review, 11(3) November 1996.

[6] White, J. E. "Telescript Technology: Mobile Agents", General Magic White Paper, 1996

[7] "Intelligent Agents : An Emerging Technology for Next Generation Telecommunications", INFOCOM96