이동 에이전트를 이용한 지역 네트워크 단위에서의 컴퓨터 바이러스 탐지 및 치료방법 구현

최종욱° 김영균 오길호
금오공과대학교 컴퓨터공학부
{jwchoi, ygkim, gilho}@cespc1.kumoh.ac.kr

A Design and Implementation of A Computer-virus Detection and Recovery Method using Mobile Agents on LAN

Jong-Wook Choi° Young-Gyun Kim Gil-Ho Oh
School of Computer Engineering, Kumoh National University of Technology

요 약

정보통신 기술의 발전과 인터넷 사용의 증가와 더불어 컴퓨터 바이러스 제작기법의 지능화 및 고급화로 인한 피해가 확산되고 있다. 따라서 이러한 컴퓨터 바이러스 피해들로부터 네트워크나 시스템을 보호하기 위해서 여러 가지 방법들과 그에 따른 시스템들이 적용되고 있다. 그러나 기존의 방법들에 대한 관리와 사용을 위해서는 사용자의 많은 작업과 비용 그리고 시간이 소요된다. 따라서 본 논문에서는 기존의 방법과 비교하여 지역 단위 네트워크 내에서 동적이고 자율적으로 이동할 수 있는 이동 에이전트를 이용하여 신속하게 새로운 바이러스에 대한 탐지와 복구기능을 수행 할 수 있는 이동 에이전트 기반의 바이러스 탐지 및 치료 방법을 새롭게 제안한다.

1.서론

최근 인터넷 기반의 환경에서 바이러스나 해킹 등의 보안 위협 요소는 점차 다양화, 지능화 되고 있으며, 사용이 간단한 도구들이 배포되어 인터넷을 통해 대량 유포되면서 인터넷상의 호스트들의 바이러스 침입은 더욱 위협을 받고 있다. 이러한 바이러스는 인터넷 사용이 급속히 확산됨에 따라 그 피해 또한 기하 급수적으로 늘어가고만 있다. 이런 바이러스를 퇴치하기 위한 기존의 상업용 백신의 대부분은 파일 시스템에 저장된 이후에 사용자나 시스템 관리자에 의해 검사되는 선 저장-후 검사 방법이므로 바이러스의 침입에 적극적으로 대응하지 못하는 수동적인 방법이기 때문에 신종 바이러스에 신속하게 대응하지 못하는 문제점이 있다. 이에 본 논문에서는 사용자 어플리케이션에 이동성을 제공하고 분산 컴퓨팅 환경 내에서의 노드들을 순회할 수 있는 지능적인 이동 에이전트(Mobile Agents)[1]를 사용하여 보다 실시간으로 그리고 능동적이며 자율적인 방법으로 바이러스를 탐지 및 복구 할 수 있는 방법을 새롭게 연구하였다. 본 논문에서 제안한 방법은 좀 더 효율적으로 네트워크 상에서 유입되는 바이러스들의 진단 및 치료를 수행할 수 있다.

2.이동 에이전트와 컴퓨터 바이러스

2.1 이동 에이전트

에이전트(Agent)란 사용자를 대신하여 사용자가 원하는 어떤 업무를 수행해주는 프로그램이라 정의 할 수 있으며 이동 에이전트는 자율성을 가지고 비동기적으로 수행이 가능한 개체로, 선택적으로 지능을 가지고 특정 작업을 수행하기 위해(본 논문에서는 바이러스 탐색 및 치료) 한 호스트에서 다른 호스트로 이동할 수 있는 개체라고 정의 할 수 있다[2]. 네트워크 상의 호스트는 에이전트가 실행 할 수 있는 환경을 제공하는 Agent system 이며 전송된 에이전트는 호스트와 독립적으로 자신의 주어진 역할을 수행할 수 있다. 작업을 완료한 에이전트는 자기 자신을 다른 호스트로 전송할 수 있으며, 복사본(clone)을 만들거나 다른 에이전트와의 통신을 하며 작업을 수행하고 모든 작업이 완료된 에이전트는 스스로를 제거할 수 있는 기능을 수행한다[3][4].

본 논문에서는 기존의 컴퓨터 바이러스 탐색 및 치료의 단점을 보완할 수 있는 방법으로 분산환경 내에서 한 호스트에서 다른 호스트로 이동하며 자율성과 지능성이라는 특성을 가지고 있는 이동 에이전트를 이용하여 바이러스를 탐지하는 기능을 가진 이동 에이전트가 각 호스트를 방문하여 바이러스를 탐지하고 탐지 즉시 사용자가 모니터링 함과 동시에 또 다른 이동 에이전트(Vaccine Mobile Agents)를 이용하여 치료를 수행하는 방법으로 새로운 바이러스에 신속하게 대응할 수 있는 장점을 제공한다.

2.2 컴퓨터 바이러스

바이러스[5]들을 탐색 및 치료할 수 있는 기존의 분산 환경 내에서의 백신 프로그램 사용환경은 새로운 바이러스에 대한 대처 방안이 수동적이고 시스템 사용자가 직접 신종 바이러스에 대한 백신 프로그램을 직접 다운로드 받아 설치해야 한다는 단점을 가지고 있다. 좀더 개선된 방안으로 방화벽 시스템의 고유의 기능을 유지하면서 네트워크 상에서 유입되는 파일의 바이러스 진단 및 치료의 과정을 수행 할 수 있는 네트워크 방화벽 시스템을 구현한 연구도 있다[6]. 이 방법 또한 바이러스에 감염된 파일을 전송 받을 경우 파일 전송 후 바이러스 감염사실을 사용자에게 통보하여 사용자로 하여금 바이러스를 치료 후 사용하거나 삭제를 요청하는 완벽한 자율성을 지원하지 못한다는 단점을 가지고 있다.

3.구성 및 동작 특성

이동 에이전트를 이용한 바이러스 탐색 및 치료 시스템의 구성은 JAVA기반 환경인 자율성(Autonomy),이동성(Mobility),상호 운용성(Interoperability)을 갖춘 다중 에이전트 시스템인 IBM Aglets system 1.1b3[7]을 사용하였다.

동작 특성은 지역 네트워크 내의 하나의 특정 호스트나 동시에 모든 호스트들에게 이동 에이전트를 파견하여 주기적으로 바이러스 유무를 판별한 후에 해당 호스트의 바이러스 정보를 중앙의 백신 에이전트 서버 시스템에 전송한다.백신 에이전트 서버 시스템은 탐지된 바이러스 정보로부터 해당 바이러스

를 치료할 수 있는 VMA(Vaccine Mobile Agent)를 바이러스에 감염된 호스트에 전송함으로써 바이러스를 치료한다. 이러한 특성으로 인해 사용자들은 바이러스 감염 여부와 치료에 대한 부담을 줄일 수 있다는 장점을 가지고 있다.

3.1 시스템의 구성

시스템의 구성은 VMAS(Vaccine Mobile Agent Server),SMA(Scanner Mobile Agent),VMA(Vaccine Mobile Agent),VIDB(Virus Information DataBase)로 구성되어 있으며 각각의 역할은 다음과 같다.

•VMAS(Vaccine Mobile Agent Server)

모든 바이러스 정보와, 해당 바이러스에 대한 치료를 할 수 있는 이동 에이전트를 저장하고 있으면서 각각의 에이전트를 지역 네트워크내의 노드들에게 파견하고 이동 에이전트들이 탐색한 결과 정보에 따른 백신 프로그램을 해당 노드들에게 전송하는 기능과 신종 바이러스에 대한 백신 프로그램을 업데이트 및 유지하는 기능을 수행한다.

•SMA(Scanner Mobile Agent)

VMAS로부터 파견되어지며 바이러스 패턴코드를 저장하고 있으며 지역 네트워크상의 호스트들에 파견 되어져 해당 호스트내의 모든 파일을 탐색해 자신의 바이러스 패턴코드 정보를 이용하여 바이러스를 탐지하며 발견되어진 바이러스 정보에 대한 백신 프로그램을 VMAS에게 요구하는 기능을 수행한다.

•VMA(Vaccine Mobile Agent)

SMA로부터 전송되어진 호스트 위치와 그 호스트의 바이러스 정보에 따른 백신코드를 가지고 VMAS로부터 파견 되어져 해당 호스트로 이동하여 바이러스를 치료하는 기능을 수행한다.

•VIDB(Vaccine Information DataBase)

모든 바이러스 정보(바이러스 패턴 코드, 감염 증상, 치료방법)를 저장하며, 탐지된 바이러스를 치료할 수 있는 백신 이동 에이전트를 저장한다.

이동 에이전트를 이용한 백신 에이전트 서버 시스템의 기능별 모듈과 전체 시스템 동작 구조는 그림 1,2 와 같다.

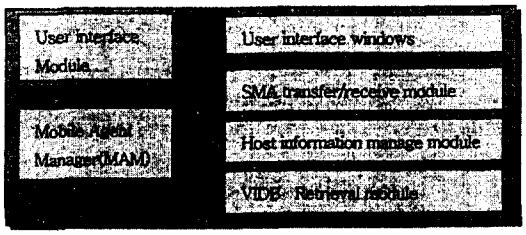

그림 1. 백신 에이전트 시스템의 기능별 모듈

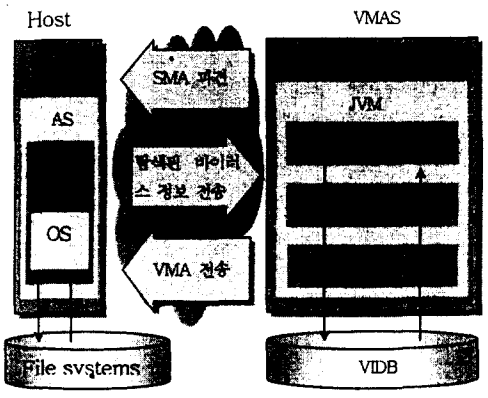

그림 2. 시스템 동작 구조

3.2 이동 에이전트를 이용한 순환 탐색 기법

이동 에이전트를 이용한 순환 탐색 기법의 전체적인 개념도는 그림 2와 같으며,다음과 같은 절차로 수행한다.

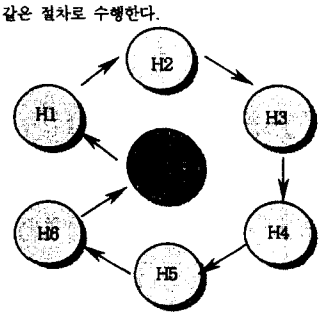

그림 3. 순환 탐색 기법

① VMAS에서 지정된 하나의 호스트로 특정 바이러스 탐색을 위하여 SMA를 파견한다.

② SMA는 해당 호스트의 파일을 검색하여 자신의 바이러스 패턴 코드와 비교하여 바이러스 유무를 판별한다.

③ SMA가 바이러스를 발견하면 해당 호스트의 위치정보와 바이러스 정보를 VMAS에게 전송하고 다른 호스트로 이동하여 바이러스 탐색을 계속 시행한다.

④ VMAS는 SMA로부터 전송 되어진 정보와 자신의 VIDB내의 바이러스 정보를 비교하여 발견되어진 바이러스에 대한 VMA를 해당 호스트로 전송하여 바이러스를 치료한다.

⑤ VMAS는 주기적으로 각각의 다른 바이러스를 탐색할 수 있는 SMA를 네트워크 내의 호스트에게 전송하여 바이러스 감염여부를 감지한다.

순환 탐색 기법에서는 독립적인 바이러스 탐색기능을 수행하는 이동 에이전트를 특정 호스트에 파견하여 그 호스트로부터 다른 호스트로 이동하면서 순환적으로 바이러스를 탐색하는 방법을 구현함으로써 하나의 이동 에이전트가 지역 네트워크 내 모든 호스트의 파일시스템을 검색, 이동하면서 바이러스 탐색기능을 수행 하기 때문에 네트워크 트래픽이 적다는 장점을 가지고 있으며 그에 반해 하나의 이동 에이전트가 순차적으로 호스트들 사이를 이동하면서 바이러스를 탐색함으로써 지역 네트워크 내의 호스트를 탐색하는 시간이 증가한다는 단점이 있다. 이러한 단점을 보완하기 위하여 이동 에이전트를 각각의 호스트들에게 동시에 전송하여 병렬적으로 바이러스를 탐색할 수 있는 기법을 이용할 수 있다.

3.3 이동 에이전트를 이용한 병렬 탐색 기법

이동 에이전트를 이용한 병렬 탐색 기법은 그림 4와 같으며 다음과 같은 절차를 수행한다.

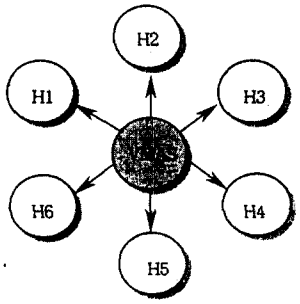

그림 4.병렬 탐색 기법

① VMAS는 지역 네트워크 내의 각각의 호스트로 바이러스 탐색을 위하여 SMA를 동시에 파견한다.
② SMA는 해당 호스트의 파일을 검색하여 바이러스 유무를 판별한다.
③ SMA가 바이러스를 발견하면 해당 호스트의 위치와 바이러스 정보를 VMAS에게 전송한다.
④ VMAS는 SMA로부터 전송 되어진 정보와 자신의 VIDB내의 바이러스 정보를 비교하여 발견되어진 바이러스에 대한 VMA를 해당 호스트에게 전송하여 바이러스를 치료한다.
⑤ VMAS는 주기적으로 바이러스를 탐색할 수 있는 SMA를 네트워크 내의 호스트에게 동시에 전송하여 바이러스 감염여부를 감지한다.

바이러스 탐색을 위하여 지역 네트워크내의 호스트들로 SMA를 동시에 파견함으로써 탐색시간을 줄일 수 있다는 것이 순환 탐색 기법과 비교하여 장점이며 SMA가 동시에 지역 네트워크 내의 모든 호스트들로 파견됨으로써 지역 네트워크내의 트래픽이 증가한다는 단점이 있다.

4.결과 및 평가

본 논문의 구현에서는 8대의 호스트의 파일에 2의 배수만큼의 host에 특정 파일에 바이러스를 감염시키고 바이러스 탐색시간 및 치료시간에 대한 성능 평가를 측정하였다. 단 본 논문의 실험에 있어서 순환탐색기법과 병렬탐색기법의 공정한 성능 평가를 위해서 모든 호스트의 동일한 디렉토리의 특정 파일에 동일한 바이러스가 감염되었다는 실험 환경을 전제로 하여 성능 평가를 하였다. 실험에 사용할 8대의 호스트에는 IBM Agent system인 Aglets 1.1b3와 자바 개발도구 JDK(Java Development Kit)1.1.8버전을 설치하여 사용하였으며 각 호스트에 파견되어 바이러스의 특정 패턴코드를 검색하기 위하여 자바 API에서 제공되는 입출력 관련 스트림 클래스들과 이 클래스에서 제공되는 메소드를 이용하여 SMA를 구축하였다. SMA는 각 호스트의 파일 시스템 정보를 얻어 해당 호스트의 파일 시스템내의 모든 디렉토리 및 파일을 읽는 동시에 자신이 가지고 있는 특정 바이러스 패턴 코드와 비교하여 동일한지 확인하는 절차를 수행하며 동일한 패턴코드가 발견되면 그 호스트의 정보 및 파일시스템의 정보를 VMAS에게 전송 후 바이러스 감염 파일을 치료 및 삭제 하도록 하였다. 지역 네트워크 내의 트래픽과 서로 다른 이질적인 성능을 가진 host에서의 바이러스 탐색 및 치료 시간의 차이를 감안하여 여러 번 실험한 탐색시간의 평균을 낸 결과는 그림5와 같이 순환 탐색 기법을 사용한 바이러스 탐색 및 치료시간에 대한 성능평가 결과는 지역네트워크 내의 바이러스 감염 노드수가 증가함에 따라 탐색 시간 또한 1.5~1.6 배정도 탐색 시간의 차이가 난다는 것을 확인할 수 있었고 병렬 탐색 기법을 사용하였을 때의 성능 결과는 1.2~1.3 배정도의 거의 아래의 그림에서처럼 거의 미미한 차이를 나타내어 바이러스 감염 노드 수에 크게 영향을 받지 않음을 확인할 수 있었다.

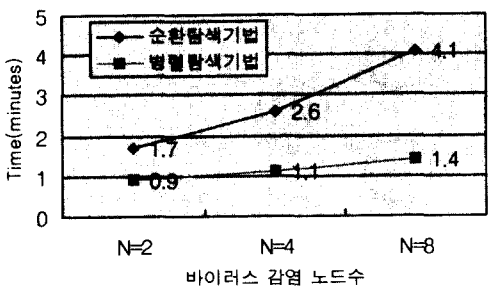

그림 5. 바이러스 감염 노드수에 따른 각 탐색기법의 성능평가 결과

표1. 감염 노드 수 와 실험 횟수에 따른 각 탐색기법의 성능평가 결과

바이러스 감염노드 수	실험횟수	탐색 시간 (minutes)			
		순환 탐색 기법	평균 시간	병렬 처리 기법	평균 시간
2*N	1	1.5	1.7	0.8	0.9
	2	1.6		1.2	
	4	1.3		0.7	
4*N	1	3.2	2.6	1.3	1.1
	2	2.9		1.2	
	4	2.1		0.8	
8*N	1	4.9	4.1	1.0	1.4
	2	3.8		1.7	
	4	3.5		1.5	

5.결론 및 향후 계획

본 논문에서 설계 및 구현된 이동 에이전트를 이용한 바이러스 탐지 및 치료 기법은 신종 바이러스에 대해 신속하게 대응하지 못한 기존의 방법과는 달리 지역 네트워크 내에서 바이러스 탐지 및 치료방법을 이동 에이전트의 특성인 자율성과 지능성을 이용하여 좀더 효과적으로 바이러스를 탐지 및 치료할 수 있도록 설계 및 구현하였다.이를 이용함으로써 날로 증대되고 있는 바이러스의 침입과 그에 따른 피해에 대해 시스템 관리자 및 사용자는 수동적이고 정기적인 바이러스 검사 방법에서 벗어나 실시간으로 바이러스 탐지 및 치료를 행할 수 있음으로 보다 신속하게 바이러스 피해에 대해 대처할 수 있다. 향후 계획은 보다 지능적인 방법으로 바이러스에 대처 할 수 있는 이동 에이전트 기반에서의 탐색 및 치료 방법과 VIDB를 효율적으로 구축 할 수 있는 방법을 연구하겠다.

참고 문헌

[1] *Vu Anh Pham, Karmouch, A.* " Mobile software agents: an overview" , IEEE Communications Magazine, Volume:36 Issue:7, July 1998
[2]Mobile Agent System Interoperability Facilities Specification, OMG TC Document. Orbos/97-10-05
[3] *Luis Moura Silva, Guilherme Soares, Paulo Martins, Victor Batista, Luis Santos,* "The Performance of Mobile Agent Platforms " ASA/MA'99, Palm Springs, California, October 1999
[4]*Danny B.Lange , Mitsuru Oshima ,* " Programming and Deploying Java Mobile Agents with Aglets"
[5]*권석철,* " 컴퓨터 바이러스 기술 동향 및 대응 전략" , 2001 국제 컨퍼런스 IT21-정보처리학회 pp.287-316, 2001.6
[6]*권석철,* " 네트워크상의 바이러스 탐지를 위한 방화벽 시스템 설계 및 구현" 2001 한국정보처리학회 춘계 학술발표 논문집 제8권 제 1호
[7]Aglets software Development kit, http://www.trl.ibm.com/aglets/