병렬처리 서버에서 실행되는 안티바이러스 엔진의 설계

유주영*, 최주영, 김미애, 박유미, 박은옥, 최은정, 김윤정, 김명주

서울여자대학교 대학원 컴퓨터학과

Design of AV Engine executed on Parallel Processing System

Ju-Young Yoo*, Ju-Young Choi, Mi-Ae Kim. Yu-Mi Park,

Eun-Ok Park, Eun-Jeong Choi, Yoon-Jeong Kim, Myuhng-Joo Kim

Department of Computer, Seoul Women's University

요 약

컴퓨터 바이러스 문제에 대한 해결 주체는 현재의 클라이언트 중심에서 서버 중심으로 옮겨가는 것이 바람직하다. 그러나 지금까지 나온 서버용 안티바이러스 엔진들은 기존의 클라이언트용 엔진에 대한 반복 구현적인 성격이 강했기에 서버 시스템 자체의 특성을 충분히 감안하지 못하고 있다. 본 논문에서는 대부분의 서버들이 다수의 CPU를 가진 병렬처리 시스템임을 감안하여 이러한 특징을 반영하여 전체적인 시스템 효율성을 높이도록 새로운 안티바이러스 엔진을 설계한 후 현재 구현 중인 주요 연구 내용을 소개한다. 다중프로세서 시스템에서 실행되는 안티바이러스 엔진은 하나의 모니터링 모듈에 다수의 동등한 에이전트 엔진을 가지고 구성된다. 모니터링 모듈은 엔진의 설치와 동적 부하균형, 자동갱신 등의 일을 담당한다. 에이전트 엔진들은 안티바이러스 기능을 기반으로 다양한 실행패턴을 가질 수 있으며 이를 통하여 서버에서 수행되는 효율성을 높일 수 있게 해준다.

I. 서론

컴퓨터 보급률의 증가와 더불어 인터넷 사용자의 증가 또한 기하급수적으로 증가하고 있다[1]. 과거, 컴퓨터 바이러스 감염으로 인한 보안상의 문제는 플로피 디스크를 경로로 한 일부 PC에 국한되어 있었다. 그러나 최근에는 이동코드 형태의 프로그램의 개발과 보급이 확대되면서 네트워크를 기반으로 한 인터넷을 통하여 생물학적 바이러스처럼 컴퓨터바이러스 또한 자가 복제, 자가 번식이 가능함으로, 단시간에 전 세계의 컴퓨터들을 무용지물로 만들어 버릴 수 있는 전염성을 갖추게 되었다[2][3]. 이에 바이러스에 대한 연구와 안티바이러스(AV) 엔진의 개발 필요성이 연구되고 있다.

현재 바이러스에 대한 대응방법으로, 일반·클라이언트들에게 제시되는 것은, PC에 설치된 AV 엔진의 정기적인 갱신(update), E-mail 사용 시 인터넷 익스플로러의 보안설정, 첨부파일 열기 전에 바이러스 체크, 중요 데이터에 대한 정기적인 백업 등을 권고하고 있다[4]. PC의 보안문제를 클라이언트 사용자인 개인에게만 넘긴다는 것은 무책임한 대응방법이다. 바이러스 감염에 대한 대응방법 개선에 있어, 클라이언트들을 위해 인터넷 관련 서버 상에서의 접근 필요성과, 서버용 AV 엔진 개발의 필요성이 있음을 알 수 있다.

본 논문에서는 이런 엔진의 필요성에 서버용 AV 엔진을 개발하려고 한다. 현재 국내외 AV 엔진 개발 업체들도 서버용 AV 엔진을 출시해서 판매하고 있다. 기존 서버용 엔진과는 달리 성능향상을 위한 서버용 엔진 설계를 제안하려고 한다. 이에 2장에서는 서버용 AV 엔진에 대한 국·내외의 관련업계의 제품들을 알아보고, 3장에서는 서버의 특징인, 멀티프로세싱 방식이란 특징을 살려서 설계에 적용함으로 그 수행 능력을 높일 수 있는 AV 엔진 설계를 제안하고, 4장에서는 결론과 향후연구방향에 대해 서술하고 맺도록 한다.

II. 국내외 서버용 AV 엔진 현황

1. 국내의 서버용 AV 엔진

국내 안티바이러스 업체로는 Everyzone, 안철수연구소, 하우리, 뉴-테크웨이브, 세종정보기술, 훈시큐어가 있다[5][6][7][8]. 이들 업체 중에 서버용 엔진은 Everyzone의 제품으로 터보백신 Manager, 터보백신 Windows Server가 있고[9], 안철수연구소에서 개발 된 제품으로는 V3 Net for Windows Server SE, V3 VirusWall File Scan, V3 NetScan2001이 있고[10], 하우리에서 개발된 제품으로는 바이로봇 Management Server, 바이로봇 Advanced Server, 바이로봇 Unix Server, 바이로봇 Linux Server, 바이로봇 for Windows IIS가 있다[11].

국내 회사에서 개발해서 판매하고 있는 서버용 AV 엔진에 대한 시스템 요구사항, 제품의 특징과 다중 cup에 대한 지원 유무는 아래 표와 같다. 표 1은 Everyzone의 터보백신 Manage와 안철수연구소의 V3 VirusWall File Scan 제품에 관한 정보이다.

표 1: EVERYZONE과 안철수 연구소의 서버용 안티바이러스 엔진

제품명		터보백신Manager	V3 VirusWall FileScan	
제품개요		에이전트의 그룹별 관리·원격제어 통합 자산관리 솔루션	기업 환경에 적합한 유연한 서버 방역 솔루션	
시스템 요구사항	CPU	인텔펜티엄급 이상의 IBM 호환 PC		
	RAM	최소 128MB, 256MB 이상 권장	256MB 최소	
	HDD	40MB 이상의 여유 공간	설치를 위한 30MB 저장 공간 압축 파일 처리를 위한 최소 200MB 공간	
	운영체제	Windows 2000 Professional 2000 Server/ XP/ NT 4.0 이상	<Unix>	Solaris SPARC 2.5/2.5/7/8 Solaris x86 2.5/2.6/7/8 AIX 4.3.3/5.x HP-UX 10.20/11.00
			<Linux>	RedHat 6.2/7.x/8.0 SuSE 7.0/7.1 Debian 2.2 Turbo 6.1/6.5
제품특징		· 중앙 집중형 원격 방역 서비스 제공 · 모듈별 업데이트 기능 · 직관적인 인터페이스 제공 · 에이전트 PC 상태보고 · 다양한 경보 서비스 · 상세한 보고서 · 부가 서비스 기능	· 정확한 바이러스 진단/치료 기능 · 효율적인 수동 및 예약 검사 기능 · 사용자 편의를 고려한 효율적인 관리 기능	
다중 CPU 지원 유무		x	x	

2. 국외의 서버용 AV 엔진

국외 안티바이러스 업체도 각 나라마다 존재하지만 본 논문에서는 시만텍과 트랜드 업체만을 대상으로 하였다. 표2는 시만텍의 AntiVirus Command Line Scanner 1.0과[12] 트랜드의 ServerProtect for Linux[13]에 관한 정보이다.

표 2: Symantec과 TrendMicro 서버용 안티바이러스 엔진

제품명			AntiVirus Command Line Scanner 1.0	ServerProtect for Linux
제품개요			Windows, Linux, Unix를 기반으로 하는 바이러스를 치료하는 높은 실행력	리눅스 서버의 효율적인 안티바이러스 관리를 위한 솔루션
시스템 요구사항	CPU		windows, Linux (펜티엄Ⅲ 이상) / Unix (400MHz 이상)	펜티엄 Ⅱ 이상
	RAM		256-512MB	128MB 이상
	HDD		8GB 이상	/opt 디렉토리용 150MB 공간
	운영체제	Windows	Windows NT SP 6 이상 Windows 2000 SP 2 이상 Windows NT Server 4.0 Windows 2000 Server	<Linux> RedHat 6.2 이상
		Linux	RedHat 6.2 이상	
		Unix	Solaris 2.6 이상	
제품특징			· 높은 이식성 · 바이러스 정보/ 엔진 자동 업데이트 · 웜, 바이러스, 트로잔, 압축파일등 방역	· 웹 브라우저를 통한 원격관리 · 고성능 바이러스 검색과 패턴 업데이트 · 로그 보고서와 이벤트 통보
다중 CPU 지원 유무			x	x

3. 국내외 서버용 AV 엔진 현황에 대한 분석

서버용 AV 엔진 제품들이 공통으로 제시하는 특징들은 아래와 같다.

1. 실시간 감시 기능
2. 업데이트(update) 기능
3. 다양한 압축 파일 검사 기능 제공
4. 사용자 사용이 편한 인터페이스 제공

공통되는 특징들은 AV 엔진으로 가져야 할 특성들이다. 표1과 표2와 같이 AV 엔진이 서버용이지만, 서버가 갖고 있는 다중 CPU에 대한 지원은 현재는 없다는 것을 알 수 있다.

III. 서버용 AV 엔진 설계

2장에서 언급했던 것처럼 현재 안티바이러스엔진으로 서버용과 클라이언트용이 갖는 특징에는 큰 차이가 없음을 보았다. 본 논문은 서버가 갖고 있는 특징 중 하나인 병렬처리를 서버용 AV 엔진 설계에 적용시켜 보려고 한다. n개 이상의 CPU를 지닌 서버일 경우, AV 엔진 작동 시 각각의 CPU를 제어하는 모니터가 필요할 것이다. 이 모니터로 n개의 CPU를 제어함으로 엔진작동을 병렬처리한다.

1. 병렬처리 서버용 AV 엔진 설계

본 논문에서 설계하는 서버용 AV 엔진의 동작 원리는 기존의 방식과 흡사하지만 다수의 프로세서를 제공하는 병렬처리 시스템에서 수행된다는 측면에서 이를 활용하는 방식에서 차이가 생긴다. 다음 그림1은 n개의 CPU를 가진 병렬처리 시스템에서 AV 엔진이 설치된 모습을 보여준다.

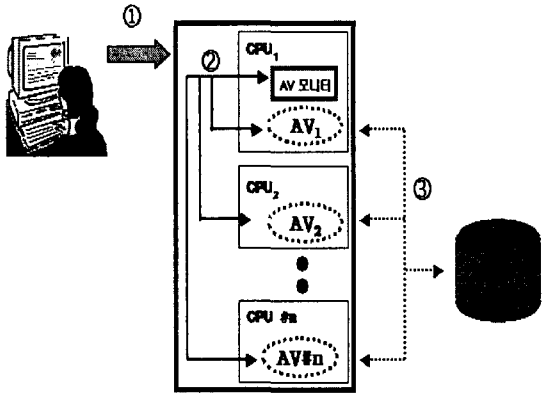

그림 1: 서버용 AV 엔진 설계

전체 n개의 CPU에 다음과 같은 형태로 설치 운영된다.

① CPU 1(일종의 마스터 프로세서)에 모니터링 모듈을 설치한다.

② CPU 1을 포함하여 CPU n까지 독립적인 안티 바이러스 엔진을 설치한다. 이러한 초기 설치는 모니터링 모듈을 통해서 이루어진다. 이 엔진은 클라이언트용 AV 엔진과 유사하다.

③ 바이러스 감지용 시그너쳐 데이터베이스(signature database)를 각 프로세서에 로딩 한다. 원래 이 데이터베이스는 모니터링 모듈이 하드디스크에 저장되어 자동 갱신 등으로 관리하지만 각 CPU의 AV 엔진이 수행될 때 지정된 실행 패턴에 따라 필요한 부분만을 캐시로 읽어 들인다. 이러한 시그너쳐 데이터는 캐시 일관성의 대상이 아니다.

④ 사용자는 초기 실행 지시를 받은 모니터링 모듈은 주어진 실행 지침 안에서 각 프로세서의 부하상태를 동적으로 체크하여 적절한 실행 패턴을 결정하여 에이전트들의 실행을 지시한다.

⑤ 각 에이전트들이 수행하여 생성된 결과는 모니터링 모듈로 전달되어 종합된 후 보고 되어진다.

실행패턴은 기본적으로 다음 2개를 토대로 하여 결정된다.

[패턴 1] 검사영역 분할형 실행패턴

검사영역을 에이전트의 개수만큼 나누어 중첩됨 없이 할당한 후 독립적으로 바이러스 검사를 수행하게 한다. 모든 에이전트는 주어진 검사영역에 대하여 모든 바이러스에 대한 시그너쳐 검사를 실시한다. 만일 특정 에이전트가 수행되는 CPU에서 부하가 임계치 이상 발생하면 해당 에이전트는 비활성화 된 후 자신의 검사영역 맵 정보가 다른 에이전트로 이동 병합된다. 이러한 부하균형 작업은 모니터링 모듈이 담당한다. 최악의 경우 하나의 에이전트가 전체 검사영역을 상대로 하여 검사할 수 있는데 이것은 기존의 클라이언트 AV엔진의 서버용 버전으로 간주될 수 있다. 이론상 가장 효과적인 경우는 n개의 에이전트가 동등한 규모의 검사대상을 동시에 검사하는 경우이다.

[패턴 2] 검사대상 분할형 실행패턴

n개 에이전트에는 모든 검사영역이 중복되어 할당된다. 그러나 각 에이전트가 검사하는 바이러스의 부류(즉 검사대상)는 상이한데 이를 위하여 시그너쳐 데이터베이스도 분할 할당된다. 따라서 검사영역 입장에서 보면 1번 에이전트부터 n번 에이전트까지 스위칭되면서 서로 다른 시그너쳐에 대하여 검사를 받게 되어 일종의 파이프라인 처리가 이루어진다. 이 경우 에이전트별로 할당된 검사대상은 악성코드의 부류에 따라 결정되는데 다음은 대표적인 사례이다.

부류 1. 최근에 가장 활동하는 악성코드 부류

부류 2. 웜 바이러스 부류

부류 3. 스크립트 바이러스 부류

부류 4. 윈도우 기반 바이러스 부류

부류 5. 기타 부류(스파이웨어, 유닉스 기반 등)

부류 1의 경우 부하균형이 가장 적은 CPU(이론 상 실행기간 내 전용 CPU)에서 수행되는 에이전트에 할당하여 수행하는 것이 가장 효과적이다.

이상과 같은 두 가지 실행패턴은 다중프로세서 시스템의 부하상태에 따라 다양한 실행패턴을 형성하여 전체 성능을 향상시키도록 지정된다.

2. AV 엔진의 구현 상황

이상과 같이 설계한 AV 엔진은 현재 썬 마이크로 시스템사의 Blade 2000 SMP(Symmetry Multi Processing) 시스템 기반 서버에서 Java Thread 기반으로 개발 중이다.

표 3: 병렬처리 서버용 안티바이러스 엔진 시스템 요구사항

개발명	병렬처리 서버용 안티바이러스 엔진
개요	병렬처리를 컨트롤 하는 서버용 안티바이러스 엔진 모니터
시스템 요구사항	· 기종 : SunBlade2003 · CPU : dual-CPU SMP (Symmetry Multi-Processing)방식 · 메모리 : 2048MB · 하드디스크 : 70GB · 운영체제 종류와 버전 : Solaris8
제품특징	· 구현 언어 : Java(java 1.4.2) · 구현 방법 : AV엔진 구현 - JavaThread AV GUI - SWING · 공개소스 사용 형태 : Clam AV(http://clamav.elektrapro.com/) 에서 바이러스 DB 사용 · 전체 소스 크기 : 14,523byte
다중 CPU 지원 유무	O

현재 CPU 2개인 서버에서 기본 구현이 이루어졌으나, 차후 확장성을 고려하여 n개의 CPU에서도 동작 가능하도록 구현하였다. 여러 가지 추가 기능들은 현재 구현 중이다.

Ⅳ. 결론 및 향후 연구 방향

다수의 프로세서를 제공하는 서버 시스템에서 수행되는 AV 엔진을 설계하여 제시하였다. 이는 기존의 클라이언트용 AV 엔진의 서버로의 단순 포팅 작업과는 다른 과정을 가지고 있다. 특히 각 프로세서의 부하상태를 동적으로 모니터링하여 전체 시스템 성능을 최적화하도록 설계되었으며, 그 과정에서 AV 엔진의 특성을 반영하였다. 모니터링 모듈에서 담당하는 부하균형 기능과 실행패턴 결정 기능은 여러 가지 상황을 감안하여 좀더 구체화될 필요가 있다. 그리고 각 에이전트 모듈 자체에 대한 성능 튜닝 작업도 이루어져야 할 것이다.

현재 썬 블레이드 2000에서만 구현 중인 이 AV 엔진을 장차 리눅스와 윈도우 기반 서버에서도 구현하기 위한 연구도 추가 병행할 예정이다.

참고문헌

[1] http://isis.nic.or.kr
[2] http://www.certcc.or.kr/statistics/virus/
[3] David Harley 저, 이동표 역, Viruses Revealed, 교학사, 2002년 7월
[4] 최주영, "인터넷 서버용 병렬처리 안티바이러스 엔진 설계", 서울여자대학교 석사학위 논문, 2002년
[5] http://www.viruschaser.com
[6] http://www.hoonsecure.com
[7] http://www.virusdesk.com/Kor/index.jsp
[8] http://www.anyvaccine.co.kr/
[9] http://www.everyzone.com
[10] http://home.ahnlab.com
[11] http://www.hauri.co.kr
[12] http://www.symantec.com
[13] http://www.trendmicro.co.kr

* 본 논문은 산업자원부에서 지원하고 있는 공통핵심기반기술개발사업의 연구결과입니다. (Commonness Kernel Foundation Technology Development Work Research Program supported by Ministry of Commerce, Industry and Energy in republic of Korea)