실시간 네트웍 감시시스템(NetCop)의 설계 및 구현

윤치영, 정천복, 황선명

mrmeg@zeus.dju.ac.kr
chunbokj@hanmail.net
sunhwang@dju.ac.kr

대전대학교 컴퓨터공학과 소프트웨어공학 연구실

요 약

최근 들어 네트웍 관리 및 컴퓨터 교육의 효율을 높이기 위한 실시간 네트웍 감시 시스템에 대한 연구의 필요가 절실히 요구되고 있다. 이러한 추세에 따라 본 연구에서는 새로운 실시간 네트웍 감시 시스템을 연구 및 개발하였다.

먼저 본 시스템은 학내 망 같은 분야의 전산 수업 시 학생들의 컴퓨터를 관리, 감독할 수 있으며 학생들의 키보드나 마우스의 제어권을 획득하여 수업 시 학생들과 1 대 1 교육을 시킬 수 있다. 또한 수업 시 효율적인 전산실습 및 교육을 위해 그것의 성능을 저해하는 사용자의 유무를 체크하고 경고 메시지 및 허용되지 않은 프로그램의 실행 방지 등 사용자의 편리를 위해 제공·비치된 컴퓨터나 어떤 형태로든지 네트웍 망에 연결된 단말기의 사용범위를 실시간으로 감시, 제어 및 관리할 수 있는 기능을 제공한다. 또한 본 시스템으로 인해 네트웍 사용의 낭비를 막을 수 있고 더 나아가 컴퓨터 교육의 질을 높일 수 있으며 사용자에 더 효율적인 교육 환경을 제공할 수 있는 장점이 있다.

A Design and Implementation of Real Time Network Monitoring System(NetCop)

Chi-Young Yoon, Chun-Bok Jung, Sun-Myung Hwang

Dept. of Computer Engineering, Daejeon University

ABSTRACT

Recently, R & D about Network Monitoring System is needed to be effective network management and to improve computer education. In this work, we propose a real time network monitoring system named NetCop to improve network management and effective use. This system is designed to show any screen to one or more students in interactive learning environment. The system also provides useful functions such as monitoring students' PCs and chat. In additions, our NetCop can provide more effective learning process to students. Finally, we expect that our system can achieve high network performance and provide high educational quality to managers.

1. 서론

인터넷의 대중적인 보급과 더불어 컴퓨터 네트워크 구성 또한 빠르게 발전, 확산되고 있는 시점에서 학교 또한 사회 어느 부분에도 크게 뒤지지 않는 컴퓨터 네트워크 환경을 구축했거나 앞을 다투어 컴퓨터 네트워크 환경 구성에 힘을 쏟고 있다. 그러나 네트워크에 연결되어 있는 학교 컴퓨터들이 목적한 바에 맞게 사용되어지는가, 네트워크 환경의 컴퓨터들을 중앙에서 원할한 관리를 하고 있느냐에 대한 질문에는 아직 긍정적인 대답을 기대할 수 없는 실정이다.[1]

인터넷 환경이 이용되기 시작한 시기가 얼마 되지 않았기 때문인지 학생들의 의식 또한 아직 학문에 도움이 되는 인터넷 사용보다 오락 채팅 등의 인터넷 사용에 더 많은 비중을 두고 있는 것이 지금의 현실이다. 이런 상황에서 교내 컴퓨터 수업시간에 학생들이 수업과 관계 없는 컴퓨터의 사용을 억제하면서 교수의 수업과 관련있는 컴퓨터의 사용이 이루어지게 하고, 학생들의 공공 장소에 비치된 컴퓨터의 사용을 극대화하기 위해서 감시와 통제할 수 있는 시스템의 필요성이 요구된다.[6]

그러나 현재 학교에는 네트워크 환경에 많은 컴퓨터들을 중앙에서 어떤 컴퓨터가 네트워크에 참여하는지, 어떤 컴퓨터가 무슨일을 수행하는지, 불법적인 작업 수행시 경고 메시지 전송등 관리할 수 있는 컴퓨터 네트워크 관리 시스템이 없다. 또한 교내 컴퓨터 수업시간에 수업과 관계 없는(오락, 수업과 관계없는 인터넷 사용, 채팅) 컴퓨터 사용에 대한 관리할 수 있는 컴퓨터 네트워크 관리 시스템이 없다.

본 논문에서는 교내 컴퓨터는 교수-학습에 도움을 주는 용도로 쓰여야 하는데 오락성이 있는 비효율적인 사용이 빈번함으로 이것을 억제할 수 있는 컴퓨터 네트워크 관리시스템을 개발해여 교내 컴퓨터가 학생들의 학문 연구에 도움이 되도록 하려고 한다.

본 논문의 구성은 다음과 같다. 2장에서는 관련연구에 대하여 기술하고 3장은 제안한 실시간 감시 시스템(NetCop)의 구조와 특성을 소개하고 NetCop의 동작환경과 구현내용은 4장에서 소개한다. 마지막으로 결론과 향후 연구방향에 대해 논의한다.

2. 관련 연구

실시간 네트웍 모니터링을 위한 시스템들은 인터넷과 멀티미디어의 확산으로 학교나 회사내의 인트라넷 구축과 함께 그 필요성이 제기되고 또한 개발되어 왔다. (주)Wtech사의 iTCORE 2000 과 (주)케이아이티사의 NetOp School이 그 대표적인 예이다[7]. 그러나, 위 시스템들은 분산 네트웍 관리나 학교를 위한 실시간 강의 솔루션 등 한가지 목적에 맞게 설계가 되었기 때문에 이에 반하는 다른 면에서는 그 기능이 미비한 실정이다.[8]

본 논문의 NetCop시스템은 분산 네트웍 관리와 실시간 강의 솔루션 등 두 가지 통합된 기능을 제공하고 있으며, 이는 수업과 동시에 학생의 주의를 집중 시킬 수 있고 또한 교사가 학생의 수업 적응력을 살펴 볼수 있는 기회를 제공한다. 이와 같은 기능들은 기존의 시스템과 가장 구별되는 점이라 할 수 있다.

표 1과 표 2에서는 기존 실시간 강의 솔루션인 (주)케이아이티사의 NetOp School과의 개발 목표와 성능적, 기능적인 면을 비교 하였다.

<표 2> 개발 목표의 비교

	NetOp School	NetCop
목 표	• 교사와 학생들간 Network를 이용한 학습 효과 증대. • 교육 활용에 목적	• 감시하고 비인가된 작업을 방지하는 곳에 사용 목적 • 교육 증대에 목적 • 회사원 컴퓨터 관리 가능

<표 3> 성능·기능 비교

		NetOp School	NetCop
기능적	연결방식	• 다양(TCP / NetBios/IPX)	• TCP/IP 이용
	모니터링	• 화면 캡쳐를 통한양방향 실시간화면 모니터링	• 화면 캡쳐를 통한 단방향 실시간 화면 모니터링 • 네트웍 패킷 모니터링을 통한 패킷 분석
	채팅	• 음성/ 문자 채팅 가능	• 관리자에서 학생에게 단방향 경고 메시지 전송
	원격제어	• 학생 컴퓨터 제어 가능 • 원격 재부팅 가능	• 학생 컴퓨터 제어 가능 • 원격 재부팅 가능
	Process 강제 종료	• 제공안됨	• 경고조치/ 종료 프로그램 구분후 강제 자동 종료 가능
	관리자 유무	• 항상 담당하는 자가 있어야함	• 담당자 없이도 자동 관리 가능
			• 컴퓨터 실행 유무 확인 가능 • 프로그램 실행 유무 확인 가능
성능적		• 양방향 통신을 이용한 교육에 주 목적	• 내부적으로는 양방향이지만 외부적으로는 단방향인 관리 목적
확장성		• 버전 별 업그레이드 시스템	• 자동 업그레이드 제공 → 항상 최신 제품 제공 • 일반 회사에서도 회사원들의 컴퓨터 사용 관리에 적극 활용가능 • 사용빈도 높은 프로그램 파악하여 차후 업그레이드 대항 프로그램 선택용이 • 수업중 모범컴퓨터를 연결, 빔프로젝트를 이용한 전 학생들 관람가능

3. NetCop(Network Cop)의 구조 및 특성

3.1 NetCop의 기본동작

그림 3.1에는 NetCop의 기본적인 동작이 나타나 있다.

그림에서 알 수 있듯이 분산된 Host들로부터 등록된 프로세스는 NetCop시스템 서버를 통해 관리되고 제어할 수 있으며 또한 관리자는 1차로 서버에서 제어된 각 Host들에 대한 프로세스 정보를 모니터링하고 이를 분석하여 불필요한 사용자의 행위에 대해 서버를 통한 권고 메시지 및 실행된 프로세스의 정지 등 직접적이고도 더 강력한 제어기능을 행사할 수 있다.

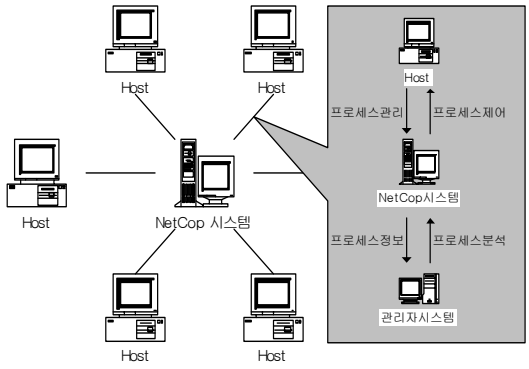

그림 3.1 NetCop 의 기본 동작

3.2 NetCop의 구조

NetCop의 구조도는 그림 3.2 와 같다.

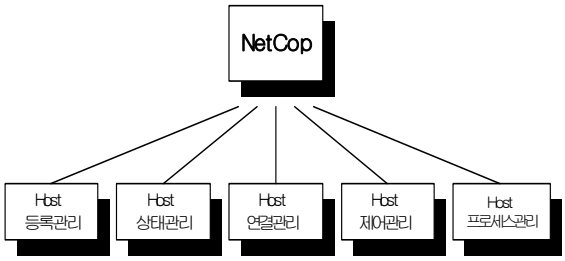

그림 3.2 NetCop 의 구조도

NetCop은 Host 등록관리, Host 상태관리, Host 연결관리, Host 제어관리, Host 프로세스관리 등 크게 다섯 개의 모듈로 구성되었다.

각 모듈별 기능은 다음과 같다.

▶Host 등록관리

관리하고자 하는 Host의 IP주소 또는 Host명을 등록하여 Host를 감시, 제어할 수 있고 또한 Host명으로도 등록가능하기 때문에 유동 IP를 채택한 네트웍 시스템에서도 사용 가능하다. 등록된 Host의 IP주소 및 Host명은 데이터베이스에 저장·관리되고 저장된 Host의 정보는 추후 허용되지 않는 프로세스의 등록 시 함께 연결되어진다.

▶Host 상태관리

각 Host의 네트웍 참여여부와 사용여부를 체크하고 또한 클라이언트 프로그램의 실행 유무를 관리하는 모듈이다.

▶Host 연결관리

클라이언트 프로그램에서 서버로의 시작을 알리는 Start 정보를 전송하고 등록된 Host의 모니터링을 위해 Host의 화면을 서버로 연결하는 등, 각 Host와의 연결을 담당하는 모듈이다.

▶Host 제어관리

1차로 서버에서 제한된 프로세스에는 포함되지 않으나 네트웍 활용을 저해하는 프로그램의 실행이나 사용자의 행위에 대해 관리자가 권고 메시지 및 마우스의 권한을 획득하여 2차로 제어를 할 수 있는 기능을 담당하는 모듈이다.

▶Host 프로세스관리

제한하고자 하는 프로그램의 프로세스를 서버에 등록하여 관리자의 모니터링을 통한 제어가 아니더라도 서버를 통해 1차 제어를 할 수 있다. 서버에 등록된 프로세스에 대해서 관리대상 Host는 그 프로세스를 실행 시 자동 종료되도록 하는 기능을 갖는 모듈이며, 여기에 등록된 프로세스 또한 등록된 Host의 정보와 연결되어 데이터베이스에 저장·관리되어 진다.

4. NetCop(Network Cop)의 구현

본 장에서는 3장에서 언급된 설계에 따라 구현된 실시간 네트웍 감시시스템(NetCop)의 구현에 대하여 소개하기로 한다.

실시간 네트웍 감시 시스템은 서버와 클라이언트 모두 Visual C++ 로 구현되었다. 클라이언트 프로그램은 특정 Host에서 백그라운드 데몬 형태로 실행되며, 서버는 관리대상 Host의 시작 시 Host로부터 서버로 보내는 Start 신호와 Host의 연결을 체크하기 때문에 서버 프로그램은 관리대상 Host가 구동되면 자동 실행되도록 되어 있다[2].

4.1 NetCop의 이벤트 제어

NetCop의 이벤트는 크게 서버를 통한 Host의 제어 이벤트와 Host에서 서버로의 모니터링 화면 전송 이벤트 두 가지로 구성된다.

그림 4.1은 서버를 통하여 Host를 제어하기 위한 패킷을 보내는 프로토콜의 모습을 보인 것이다.

Table	Var 1	Val 1	...	Var n	Val n

그림 4.1 프로토콜 구조

전송되어진 프로토콜은 변수/값의 유무에 따라 분할되어 제어기능을 가르키는 Var 부분은 반환하고 제어기능의 실질적인 값을 가리키는 Val 부분은 포인터로 연결된다. 이렇게 linkedlist에 저장된 값은 이벤트 전송의 완료시점에서 제어를 완료한다.[4].[5]

그림 4.2 는 화면 전송/저장 이벤트 위한 16bit Color 구조를 보이고 있다. 그림 3.2에서 보는 바와 같이 본 시스템에서는 화면 전송/저장 정보를 위해 16bit Color를 사용하고 있다. 예를 들어 Server와 연결이 이루어지고 Server화면이 보통 1024*768의 해상도를 가진 시스템이라면 네트워크상에서의 실시간 화면 업데이트를 위하여 100*100으로 나누어 보내게 되고 화면상의 빠른 실시간 업데이트를 위하여 JPEG 압축 코덱을 이용하여 전송한다[3]. 향후 Version-Up 시 16bit Color 이외의 시스템에서도 사용 가능하게 되어야 할 것이다.

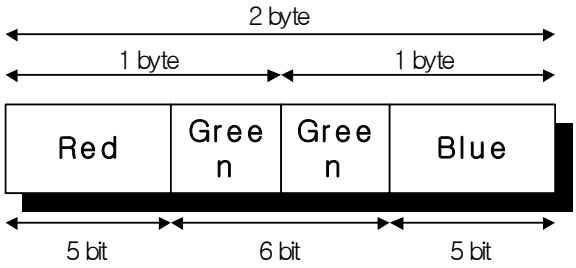

그림 4.2 전송/저장 정보를 위한 16bit Color 구조

4.2 NetCop의 서버 인터페이스

그림 4.3은 실시간 네트웍 감시시스템(NetCop)의 서버 인터페이스를 보인 것이다.

그림 4.3 서버 인터페이스

NetCop은 각 Host의 사용행위에 대해 실시간 모니터링을 통하여 감시, 관리된다. 그림 4.3에서 보는 것과 같이 관리자는 관리대상 Host를 등록관리하고 관리대상 Host의 리스트 화면에서 등록된 Host의 연결여부, 네트웍 참여여부 및 클라이언트 프로그램의 실행여부를 실시간으로 Update하여 보여준다. 또한 관리자는 사용자의 Host사용행위에 대해 실행을 제한할 프로세스를 등록·관리할 수 있고 여기에서 등록된 프로세스는 Host에서 실행 시 자동 종료된다. 이와 같은 자동종료 기능은 감시 및 관리되는 많은 Host들에 대해 각각 개별 제한해야 하는 불편함을 없애고 서버에 한번만 등록함으로서 등록된 Host들을 제어할 수 있는 기능이다. 그리고 관리자는 개별 Host의 사용행위에 대한 사용화면을 실시간 모니터링 함으로써 1차로 제한된 프로세스의 목록에는 포함되지 않으나 그 사용범위가 불필요한 사용행위로 간주 될 때에는 직접 Host의 권한을 획득함으로써 제어를 할 수 있다.

그림 4.4 원격지 Host에 대한 권고메시지

그림 4.5 원격지 Host에 대한 권한 획득

그림 4.4 와 그림 4.5 는 서버로부터 관리대상 Host로의 권고 메시지 및 Host에 대한 마우스, 키보드의 권한을 획득하여 제어를 가하고 있는 화면을 보인것이다. 허용되지 않는 프로세스의 목록에는 포함되지 않으나 관리자의 실시간 모니터링을 통하여 불필요한 행위일 때는 가벼운 권고 메시지 및 Host의 마우스, 키보드의 권한을

획득하여 직접 Host를 제어할 수 있고 특별한 경우에는 Host를 리 부팅 시킬 수 있다.

4. 결론 및 향후 연구 방향

본 논문에서는 무분별한 사용자의 Host 및 네트웍 사용을 원격에서 감시 및 제어할 수 있는 실시간 네트웍 감시시스템(NetCop)을 구현 연구하였으며 이러한 시스템은 교수-학습의 편리를 위해 제공·비치된 컴퓨터나 어떤 형태로든지 네트웍 망에 연결되어 학습에 사용되는 단말기의 사용범위를 실시간으로 감시, 제어 및 관리할 수 있는 기능을 제공함으로써 다음과 같은 효과를 기대할 수 있다.

첫째, 특정 학생으로 인한 교육 분위기의 저하를 막을 수 있기 때문에 다수의 학생에게 더 효율적인 교육 환경을 제공할 수 있으며 더 나아가 교육환경의 전체적인 성능을 높일 수 있게 될 것이다. 둘째, 다수의 원격지 Host를 서버에서 관리, 제어할 수 있기 때문에 전산실습 및 컴퓨터를 이용한 수업시 학생들과의 1 대 1 교육환경을 제공할 수 있을것이다. 셋째, 기밀을 필요로 하는 프로젝트를 진행하는 회사나 학교같은 교내망을 설치,이용하는 환경에서의 관리 응용도 기대해 볼 수 있다.

현재 구현된 시스템은 서버와 클라이언트가 수시로 패킷을 교환해야 하기 때문에 오히려 이로 인해 생기는 네트웍의 과부하는 고려하지 않은 실정이며 또한 한번에 하나의 Host 화면만 모니터링하기 때문에 관리자의 계속적인 모니터링이 필요하고 그것을 벗어난 Host는 제한된 프로세스 이외의 행위에 대해서는 무방비 상태에 놓인다는 단점이 있다.

Host들에 대한 계속적인 실시간 모니터링을 하면서도 네트웍에 대한 부담을 줄이고 제한하기 위해 등록하는 프로세스 이름 대신 사용자가 더 쉽게 알 수 있는 것으로 대체할 수 있는 연구를 수행하는 것이 필요할 것으로 생각된다.

【 참 고 문 헌 】

[1] 임병학, 방윤학 “효율적 인터넷 트래픽 처리를 위한 공중 가입자 인터넷 액세스 기술” 정보과학회지(99‘)

[2] Dave Bixler, Larry Chambers, Joseph Phil “Implementing and Administering a Microsoft Windows 2000 Network Infrastructure” 삼각형 프레스, 2001

[3] Alan Burns, Andrew J. Wellings “Real Time Systems and Programming Languages 3E” Addison-Wesley, 2001

[4] John G. Ackenhusen “real-time Signal Processing : Design and Implementation of signal Processing Systems” Prentice Hall, 1999

[5] Donald L. Bailey, Raymond J.A. Buhr “An Introduction to Real-Time Systems from Design to Networking with C/C++” Prentice Hall, 1999

[6] Wayne Wolf, Yiqing Liang, Michael Konzuch, Heathery Yu, and Michael Philips, ″A Digital Video Library on the World Wide Web″, ACM Multimedia96

[7] “http://www.wtech.co.kr″

[8] ″http://www.netopkorea.com″

○ 황선명
1987년 중앙대학교 전자계산학과 박사
1988년 독일 Bonn대학 Post Doctor
1989년～현재 대전대 컴퓨터정보통신공학부 부교수
관심분야 소프트웨어 품질보증, 테스팅 방법 및 도구, 표준화, 재공학

○ 정천복
1994년 청주대학교 산업경영학과 석사
2002년 대전대학교 컴퓨터공학과 박사
1991년～현재 대전여자상업고등학교 교사
관심분야 테스팅 방법 및 도구, 멀티미디어 컨텐츠

○ 윤치영
2001년 대전대학교 컴퓨터공학과 학사
2001년～현재 대전대학교 컴퓨터공학과 석사과정
관심분야 테스팅 방법 및 도구, 컴포넌트 소프트웨어