SSL을 이용한 웹기반 계층적 네트워크 관리 시스템의 설계 및 구현

황 일 선*, 이 명 선*, 유 기 성*, 김 종 근**, 조 강 홍**, 정 진 욱**
* 한국과학기술정보연구원 슈퍼컴퓨팅센터
** 성균관대학교 정보통신공학부

요 약

MSP(Management Service Provider) 사업을 위해서는 네트워크 관리 시스템은 로컬 네트워크뿐만 아니라 다른 네트워크를 통합적으로 관리하기 위해 관리 서버들 간에 정보를 주고받는다. 이때 사용되는 통신 회선은 여러 사용자가 사용하는 공유 회선이므로 제3자가 회선을 통해 전달되는 정보를 훔쳐볼 수 있다. 정보 중에는 관리자나 장비들의 중요한 정보가 포함되어 있기 때문에 이들 정보에 대한 보호가 필요하다. 일반적으로 통신 회선의 보안을 위하여 SSL(Secure Socket Layer)을 많이 사용하는데 네트워크 관리 시스템에서도 서버와 클라이언트 간에 통신이나 관리 서버들의 통신에 SSL을 사용하여 정보를 보호하고자 한다.

Design and Implementation of Web-based Hierarchical Network Management System using SSL

I-S Whang*, M-S Lee*, K-S Lyu*, Jong-Kun Kim**, Kang-Hong Cho**, Jin-Wook Chung**

ABSTRACT

Network management system exchanges information between management servers to manage other network as well as local network for MSP(Management Service Provider) business. Because communication line that is used here is communication line that several users use, other user can steal a important information that are passed through communication line. For these information include important information of administrator or equipments, These information should be protected. Usually it is use much SSL to security of communication and it wish to protect information using SSL in communication between management servers' or communication between server and client at network management system to use much SSL for security of communication.

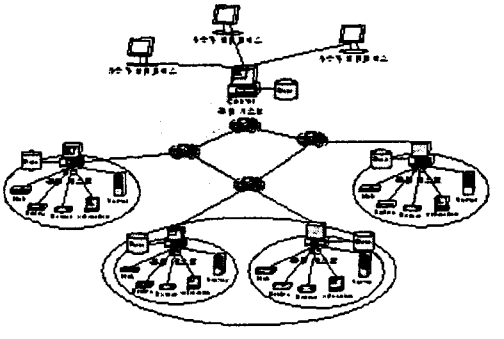
1. 서 론

네트워크의 규모가 소규모이고 네트워크에서 제공하는 서비스들이 다양하지 않았던 초기의 경우에는 네트워크 관리가 그리 문제가 되지 않았다. 그러나 네트워크의 규모가 갈수록 커지고 이들 네트워크에서 제공하는 서비스의 종류가 다양해지고 이들 서비스들 제공하기 위해서 네트워크에 요구되는 요구사항들이 늘면서 점차 네트워크 관리의 필요성이 인식되었다.[1,2,3] 지금의 네트워크 환경은 LAN(Local Area Network)상에 다양한 네트워크 장비, 서버, 워크스테이션 및 PC로 구성된 대규모의 분산된 구조를 이루고 있다. 다양한 이기종으로 구성된 고성능의 통신 기술과 강력한 기능을 보유한 서버 및 워크스테이션의 설치가 보편화 되어감에 따라 이들에 대한 효과적인 네트워크 구축과 활용, 그리고 네트워크 관리의 효율성과 비용의 절감이라는 측면에서 네트워크 관리 시스템(NMS)의 중요성이 대두되게 되었다.

이와 같이 네트워크 관리의 중요성이 대두되면서 초기의 네트워크 관리 시스템 개발에 있어서 개발자들은 사용자의 편리함과 관리자가 네트워크 관리를 효율적으로 하기 위한 기능들만을 고려하여 개발하였지 시스템에서나 통신상의 보안문제는 전혀 고려하지 않았다. 이와 같은 보안문제는 로컬 네트워크를 관리하는데는 크게 문제되지 않았다. 하지만 자신의 네트워크를 관리할 능력이 없거나 비용상의 문제로 외부의 전문 네트워크 관리 업체에 자사의 네트워크 관리를 의뢰하여 관리를 받는 MSP (Management Service Provider) 사업이 생겨나면서 로컬 네트워크가 아니 다른 네트워크와도 통신을 해야하기 때문에 문제가 되고 있다. 이와 같은 보안문제 때문에 네트워크 관리를 위해 사용하는 네트워크 관리 프로토콜인 SNMP에서는 중요한 네트워크 장비들에 대한 접근시에 인증이나 주고받는 정보들을 암호화하는 기능을 추가한 SNMPv2, v3를 지원하여 아무나 네트워크 장비에 접근하지 못하도록 하고 있다. 하지만 이것은 단지 네트워크 장비들에 대한 접근시에 인증을 해주거나 주고받는 정보를 암호화하므로 정보를 보호하는 것이지 이들 네트워크 관리 시스템 자체의 보안이나 사용자에게 정보를 보여주는 클라이언트와 네트워크 관리 서버와의 통신에 오가는 정보들을 보호하기 위한 방법을 제공하지는 않는다. 이에 본 논문에서는 많은 보안 솔루션 중에서 가장 일반적으로 사용하는 SSL을 이용한 웹기반의 계층적인 네트워크 관리 시스템의 설계 및 구현을 하고자 한다. 이를 위해 우선 네트워크 관리 구조에 대해서 살펴보고 관리 시스템에서의 보안취약 요소를 정의하도록 한다.

2. 계층적 관리 시스템

기존에 네트워크 관리 구조는 크게 세 가지 형태로 나눠볼 수 있다. 첫째는 네트워크 관리 서버가 중앙에 하나 존재하여 이 서버에서 모든 네트워크 자원들을 관리하는 형태의 중앙 집중형 구조이다. 둘째는 지역적 네트워크를 관리하는 관리 서버들과 이들 서버 위에 하나의 서버가 존재하여 서버들을 관리하는 형태의 계층형 구조이다. 셋째는 각 지역 네트워크를 관리하는 서버들이 자신의 네트워크 자원들을 관리하면서 동등한 협력 관계를 유지하는 형태의 분산형 구조이다.[4]



(그림 1) 네트워크 관리 시스템의 전체 구조

2.1 중앙 집중형 구조

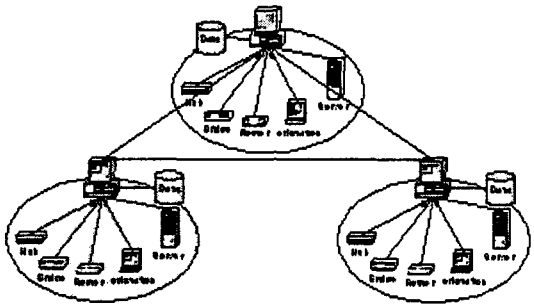
중앙 집중형 구조는 하나의 관리 서버가 모든 네트워크 자원들을 관리하는 형태이다. 이와 같은 구조에서는 중앙에 있는 관리 서버가 에이전트와의 통신, 분석, 장애 통보 및 관리자의 요청 처리 등을 담당하게 된다. 이런 관리 구조는 소규모의 네트워크를 관리할 때 가장 적합한 형태로 구현이 간단하고 모든 네트워크 자원의 상태를 한눈에 파악할 수 있다는 장점이 있지만 관리 네트워크가 커짐에 따라 중앙 서버에 걸리는 부하가 커지게 된다. (그림 1)에서 보면 하나의 지역 관리 시스템을 생각하면 될 것이다.

2.2 계층형 구조

관리 네트워크를 여러 개로 분리해서 이들 네트워크를 관리하는 보조 서버를 하나두고 이들 보조 서버들을 관리하는 메인 서버를 두므로 계층적인 형태를 갖는 구조이다. 여기서 보조 서버들은 중앙 집중형 구조에의 관리 서버와 같은 역할을 한다. 한가지 다른 점은 상위의 메인 서버로부터의 요청을 받아서 처리한다는 점이다. 또한 메인 서버가 관리하는 대상은 네트워크 자원이 아닌 보조 서버들을 관리하므로 전체적인 네트워크 관리를 원활히 수행하도록 한다. 이와 같은 구조는 관리 네트워크가 증가하여도 보조 서버를 하나 추가하므로 가능하기 때문에 확장에 유리하다는 장점이 있다. (그림 1)이 이와 같은 계층형 구조를 갖고 있다.

2.3 분산형 구조

계층형 구조에서는 보조 서버들간에 정보 교환이 없지만 분산형 구조에서는 이들 보조 서버가 자신의 네트워크를 관리할 뿐만 아니라 다른 보조 서버와도 정보를 주고받아 전체 네트워크를 관리하는 형태이다. 서로 독립적으로 운영되면서 필요한 경우 상대방에게 도움을 요청하는 형태로 하나의 보조 서버가 비정상적으로 동작하더라도 다른 보조 서버가 이를 대신하므로 지속적인 네트워크 관리를 가능하게 해준다. (그림 2)는 네트워크 관리의 분산형 구조를 보여주고 있다.



(그림 2) 분산형 구조

3. SSL을 이용한 통신 보안

기존에 네트워크 관리는 로컬 네트워크 관리를 대상으로 하여 개발되었기 때문에 통신에서의 보안 문제를 심각하게 고려하지 않았다. 하지만 네트워크간에 정보를 주고받는 분산 형태의 네트워크 관리 구조가 되면서 통신 보안은 중요한 문제로 인식되고 있다. 기존에 네트워크 관리 시스템에서 보안이 취약한 부분을 살펴보면 크게 3부분으로 나눠 볼 수 있다. 첫째는 사용자와 관리 서버사이인데 이들은 여러 사용자가 사용하는 공유회선을 사용하므로 주고받는 정보들을 제3자에 의하여 감시되거나 읽혀질 수 있다. 둘째는 관리 서버에서 관리자가 관리하고자 등록한 피관리 장비들을 관리하기 위하여 필요한 정보를 요청하고 받을 때 중간에서 정당하지 않은 제3자가 이들 정보를 훔쳐볼 수 있다. 셋째는 네트워크 관리 시스템에 저장된 장비들에 대한 정보나 관리자에 대한 정보들에 대한 유출이 있을 수 있다. 이중에서 세 번째는 시스템 보안에 해당하므로 이 논문에서는 다루지 않는다.

3.1 사용자와 관리 서버

사용자에게 정보를 보여주는 클라이언트와 네트워크 관리 서버와의 통신 회선에 해당한다. 네트워크 관리 시스템이 관리자의 이동성이나 관리 시스템에 접근을 쉽게 하기 위하여 웹 기반의 사용자 인터페이스를 제공하는데 이런 경우에 인터넷이 사용 가능하고 웹 브라우저가 설치된 로컬 시스템에서 관리 서버로의 접근이 가능하다. 문제는 인터넷이 누구나 사용할 수 있는 공유회선을 사용한다는 것이다. 이 공유회선을 통해서 관리 서버와 사용자 시스템간의 통신이 이뤄지기 때문에 회선을 통해서 흐르는 정보를 제3자가 훔쳐볼 수 있다는 것이다.

3.2 메인 관리 서버와 보조 관리 서버

네트워크 관리를 위해서는 우선 관리하고자 하는 장비들에 대한 정보를 인위적이든 관리 시스템이 자동으로 인식하든 관리 장비들을 등록하는 단계가 필요하다. 이 단계를 통해서 관리하고자 하는 장비들에 대한 리스트가 확보되면 관리 서버는 장비들에게 관리를 위해 필요한 정보를 요청하게 된다. 물론 이들 장비들은 네트워크 관리 프로토콜인 SNMP를 지원하고 있어야 한다.

네트워크 관리를 위해서는 하나의 네트워크 관리 시스템에서 모든 장비들을 관리 할 수도 있지만 지역적으로 떨어져 있거나 한 지역에 너무 많은 장비가 있는 경우에는 이들 장비들을 서로 불리하여 계층적으로 관리하게 된다. 이때 이들 관리 시스템 간에 정보를 주고받게 되는데 여기에서도 통신상에 정보유출이 있을 수 있다.

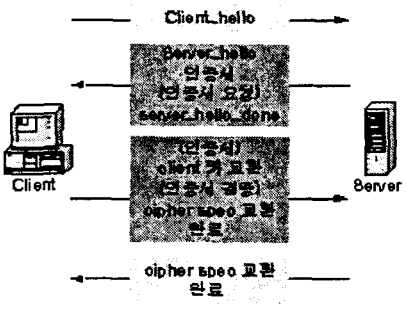
3.3 SSL의 보안기능

SSL은 TCP/IP 트래픽에서 인증과 데이터 무결성을 수행하도록 암호화하는 프로토콜이다. SSL의 최신 버전은 TLS(Transport Layer Security)라고 불리는데 TLS v1.0은 SSL v3.1과 같다.

SSL은 TCP/IP의 최상위에서 동작하고 거의 모든 종류의 소켓 통신에 적용될 수 있는데 HTTP를 안전하기 위해서 가장 많이 쓰인다. HTTP가 SSL으로 안전하게 되면 이것을 HTTPS라고 부른다. 대부분의 브라우저는 HTTPS 연결을 지원한다.

SSL은 세션키 암호화에 기반을 두고 있고 X.509 인증서와 MAC를 이용한 무결성 검사 등 몇 가지 기능이 추가되었다.

SSL은 클라이언트와 서버가 통신의 스트림을 구축하게 하는 확장 소켓이며 신원을 확립하고 키를 교환하는 handshake 과정을 거친 후에 둘 간에 통신이 시작된다. 키 교환에는 RSA, 세션키에는 RC4가 사용된다. (그림 3)은 SSL의 handshake 과정을 보여주는 것으로 handshake 동안 클라이언트와 서버는 공유 세션키를 생성하고 서로의 신원을 검증한다. 이것을 하기 위해서는 여러 메시지를 교환하여야 한다.



(그림 3) SSL의 handshake 과정

4. 계층적 관리 시스템의 설계 및 구현

네트워크 관리 시스템은 네트워크 관리를 수행하는데 기본적으로 사용자에게 정보를 제공하는 사용자 인터페이스가 있다. 이 사용자 인터페

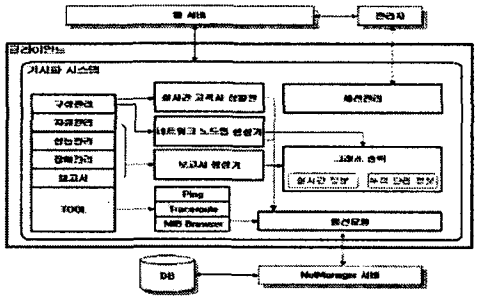
이스를 통하여 관리자나 사용자는 네트워크의 상태를 파악할 수 있고 필요한 관리 행위를 할 수 있다. 여기서는 관리 시스템이 로컬 네트워크의 관리만을 담당하는 것이 아니라 서로 다른 네트워크들을 관리 할 수 있도록 지역적으로 떨어져 있거나 규모가 큰 네트워크들을 담당하는 지역 관리 시스템을 두어 관리하도록 하는 계층적 관리 시스템 구조로 설계하였다. 그리고 이들 관리 서버들간의 통신을 보호하기 위하여 SSL을 이용하도록 설계하였다.

4.1 웹 기반의 사용자 인터페이스

관리자가 전체 시스템에 대한 관리 행위를 수행할 수 있도록 하는 인터페이스이다. 관리자는 이를 통해서 전체 시스템의 자원 정보를 검색하거나 새로운 자원을 등록, 변경, 삭제할 수 있고, 데이터 수집 주기 등의 관리정보를 설정/변경하는 관리환경설정, 그리고 전체 네트워크에 트랙픽 누적정보, 트래픽 순위별 실시간 분석정보 등의 성능관리, 장애 발생에 대한 통계정보 및 장애 로그를 보여주는 장애 관리, 지식정보관리를 통해 네트워크를 종합적으로 진단하고 새로운 지식을 입력하며 보고서 관리로 이에 대한 보고서 파일을 관리할 수 있다.

① **자원관리** : 자원을 등록하고 자원에 대한 상세 정보 등을 볼 수 있고 각 자원의 정보를 변경/삭제 할 수 있다.
② **관리환경설정** : 자원(회선, 장비)에 대한 임계값 설정 및 데이터 수집 주기를 설정할 수 있는 기능을 제공한다.
③ **성능관리** : 전체 네트워크의 성능관련 항목의 실시간(TopN 또는 LowN)정보와 누적정보를 제공한다.
④ **장애관리** : 장애관련 항복의 누적정보와 장애로그 정보를 제공한다.
⑤ **지식정보관리** : 자원(장비, 회선)의 성능 및 장애 분석 결과에 대한 관리자의 자문 보를 입력하고 입력된 이력정보를 키워드별, 조회수별, 기간별 검색기능과 이력정보의 통계정보를 제공한다.
⑥ **보고서관리** : 일정 주기로 특정 장애에 대한 보고서가 생성되도록 설정하고 생성된 보고서를 검색하는 기능을 제공한다.

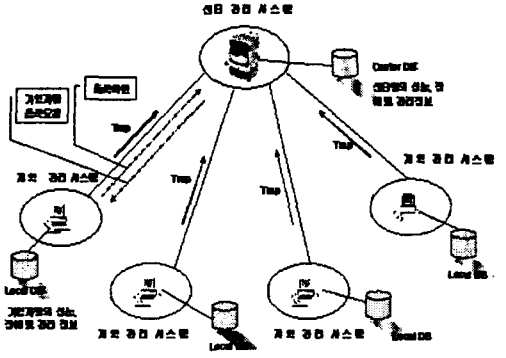
(그림 4)는 사용자 인터페이스를 제공하기 위한 가시화 시스템의 구조도를 보여주고 있다. 이 가시화 시스템은 사용자 인터페이스를 제공하고 인터페이스를 통해 요청된 명령들을 관리 서버에 전달하는 중계자 역할을 하게 된다.



(그림 4) 가시화 시스템 구조도

4.2 계층적 네트워크 관리 구조

네트워크 규모가 커지고 MSP 사업을 위해서 산재되어 있는 네트워크 자원들을 관리하기 위해서는 중앙 집중형 관리 구조보다는 전체 네트워크를 네트워크 규모나 지역적인 위치에 따라 몇 개의 소집단으로 나누어 관리하는 계층형 관리 구조가 적합하다. 이에 네트워크 전체를 관리하기 위한 네트워크 관리 시스템은 상위 시스템인 센터 관리 시스템과 그 하위에 지역 네트워크를 관리하기 위한 지역 관리 시스템(또는 가입자망 관리 시스템)을 갖는 계층형 구조로 설계하였다.



(그림 5) 계층적 네트워크 관리 시스템 구조

(그림 5)는 계층적인 네트워크 관리 시스템의 전체적인 구조를 보여주고 있다. 센터 관리 시스템과 지역 관리 시스템은 각자의 DB를 가지고 각 도메인에 대한 네트워크의 성능 및 장애 항목을 관리한다. 또한 가입자망에서 발생한 중요한 트랩 정보는 센터 관리 시스템에 전달하여 처리하도록 하였다. 그리고 가입자망의 자원을 등록시에 센터 관리 시스템에서 지역 관리 시스템으로 등록 요청을 보내며, 지역 관리 시스템에서 등록 요청에 대해 등록이 정상적으로 되면 확인 메시지를 센터 관리 시스템에게 보내므로 등록이 완료된다. 이들 센터 관리 시스템과 지역 관리 시스템들의 관리 범위와 기능에 대한 정의는 다음과 같다.

4.2.1 센터 관리 시스템

① 실시간 지역 네트워크 관리 기능

센터 관리 시스템은 지역 관리 시스템의 맨 상위의 관리 시스템으로 지역 관리 시스템을 관리하며 각 지역 관리 시스템과 연동을 통하여 지역 네트워크를 관리할 수 있는 기능을 가진다. <표 1>은 실시간 지역 네트워크 관리를 위한 기능들을 보여준다.

<표 1> 실시간 지역 네트워크 관리 기능

	기능	설명
실시간 지역 네트워크 관리 기능	실시간 트래픽 분석 기능	각 지역 네트워크의 장비를 대상으로 현재 사용하고 있는 실시간 트래픽 정보를 제공
	지역 관리 시스템과의 웹 연동 기능	웹을 통한 센터 시스템과 지역 관리 시스템의 연동 기능
	지역 관리 시스템 관리 기능	센터 관리 시스템은 주기적인 메시지 전송으로 지역 관리 시스템의 올바른 동작 여부를 관리

② 장애 탐지 기능

네트워크에서의 장애는 치명적일 수 있으므로 장애의 발생을 보다 빨리 탐지하여 필요한 조치를 수행하는 것이 중요하다. 본 시스템에서는 전체 네트워크의 장애 발생을 탐지하여 실시간으로 맵에 표시함으로써 네트워크 상태를 능동적으로 나타낸다. 관리자는 단지 전체 지역 네트워크 맵을 살펴봄으로써 네트워크의 이상 유무를 쉽게 파악할 수 있다. <표 2>는 장애 탐지를 위한 기능들을 보여준다.

<표 2> 장애 탐지 기능

	기능	설명
네트워크 장애 탐지 기능	계층별 탐지 표시 기능	센터 시스템, 즉 맨 상위 계층에 어떤 지역 네트워크의 장애인지를 표시하고, 이를 통해 지역 네트워크의 장애 발생 장비를 표시
	Trap 기반 알람 통보 기능	지역 관리 시스템으로부터 발생된 Trap을 표시하여 알람 통보
	임계값 기반 장애 탐지 기능	해당 분석 항목의 임계값을 설정하여 이를 기반으로 동적으로 장애 여부를 판단

③ 성능 분석 및 통계 정보 제공 기능

센터 관리 시스템은 지역 관리 시스템으로부터 중요한 관리 정보를 수신하여 네트워크에 대한 성능을 분석하는 기능을 제공한다. 각 관리 항목에 따라 네트워크 전체의 성능 여부를 판단할 수 있으며, 이를 기반으로 다양한 형태의 네트워크 트래픽 관련 통계 정보를 제공한다. <표 3>은 성능 분석 및 통계 정보 제공을 위한 기능들을 보여준다.

<표 3> 성능 분석 및 통계 정보 제공 기능

	기능	설명
성능 분석 및 통계 정보 제공 기능	전체 지역 네트워크 누적 트래픽 통계 정보	네트워크에 대한 각 지역 네트워크별 통계 정보와 지역 네트워크간의 트래픽 비교 분석 정보 등을 제공
	성능 Top N 기능	이용률 등의 성능 분석 항목에 대한 상위 N 개의 시스템을 탐색하여 제공하는 기능
	장애 Top N 기능	에러율 등의 장애 분석 항목에 대한 상위 N개의 시스템을 탐색하여 제공하는 기능

④ 네트워크 현황 분석보고 기능

네트워크의 성능 분석 및 통계 정보에 대한 보고서 생성 기능을 제공한다. 보고서는 보고서를 보는 관점에 따라 다른 형태의 정보가 제공될 수 있으므로, 그 보고서 출력 내용을 레벨을 두어 구분하여 제공한다. <표 4>는 네트워크 현황 분석 보고를 위한 기능들을 보여준다.

<표 4> 네트워크 현황 분석보고 기능

	기능	설명
네트워크 현황 분석 보고 기능	일/주/월 단위 보고서 생성	일/주/월 단위에 따른 네트워크의 통계 정보 생성 기능
	웹 기반 그래픽 보고 기능	다양한 그래프(표, 꺾은선, 파이)를 통해 분석 정보 출력
	계층별 보고 기능	센터 시스템의 관리자 레벨에 따른 총괄, 상세 보고서 생성 기능

4.2.2 지역 관리 시스템

① 실시간 트래픽 정보 기반 네트워크 맵 기능

계층적 네트워크 맵을 웹 상에 적용시켜 현재 네트워크 상황을 모니터링하는 기능을 제공한다. 여러 시스템들이 이와 유사한 기능을 제공하지만, 웹 상에서 네트워크 맵을 통해 트래픽 정보, 장애 탐지 정보 등을 실시간으로 제공하지 못하고 있다. 본 시스템에서 관리자는 네트워크 전체 구성을 볼 수 있으며, 마치 고속도로의 트래픽 상황을 CCTV를 통해 보는 것처럼 실시간 트래픽 현황, 장애 현황을 네트워크 맵을 통해 한 눈에 파악할 수 있다. <표 5>는 실시간 트래픽 정보 기반 네트워크 맵을 위한 기능들을 보여준다.

<표 5> 실시간 네트워크 맵 기능

	기능	설명
실시간 트래픽 정보 기반 네트워크 맵 기능	네트워크 맵 생성 기능	네트워크 관련 정보를 입력으로 하여 해당 네트워크 장비와 구성도를 자동으로 그려주는 기능
	네트워크 맵 관리 기능	그려진 네트워크 맵을 마우스 드래그를 통하여 원하는 형태로 수정하고 저장할 수 있는 기능
	실시간 트래픽 정보 표시	이용률/에러율 등 현재 각 시스템의 트래픽 정보를 표시해주는 기능
	네트워크 장비 상태 표시	네트워크 장비의 UP/DOWN 여부를 판단하여 표시해 주는 기능

② 성능 분석 및 진단 기능

네트워크 관리를 위해서는 실제로 관리자가 필요로 하는 분석 항목을 통해 진단하는 기능을 제공해야 한다. 본 시스템에서는 네트워크 관리에서 사용되는 단순 관리 정보를 추출하고 가공하여 의미 있는 성능 및 장애 관리 정보로 변환하여 제공하며, 이 과정에서 임계값, 규칙 등을 적용하여 진단하는 기능을 가진다. <표 7>은 성능 분석 및 진단을 위한 기능들을 보여준다.

<표 7> 성능 분석 및 진단 기능

	기능	설명
성능분석및진단기능	선로 이용률	선로의 사용률을 나타내는 기준이며 이 항목의 누적 분석을 통해 선로의 증/감속 여부를 판단
	입출력 패킷/바이트	네트워크 또는 시스템의 입력/출력의 패킷/바이트 값과 그 비율을 계산
	선로 에러율	네트워크를 구성하는 선로가 가지는 품질상의 문제점을 측정하는 기능
	패킷 유형별 분석	유니캐스트, 비유니캐스트 패킷 통계 분석기능
	패킷 손실율	장비의 IP 계층에서 손실되는 패킷의 비율
	패킷 폐기율	네트워크 장비의 IP 계층에서 폐기되어지는 비율
	응답 시간	응답 시간을 통한 각 시스템의 성능 정보 제공
	임계값 설정 기능	각 항목의 임계값 설정을 통하여 관리자가 자신의 관리 기준을 제공할 수 있는 기능

③ 실시간 장애 탐지 기능

네트워크 상에서 장애 발생은 가장 치명적인 문제이다. 이 경우, 먼저 장애가 발생했는지 안했는지의 장애 발생 여부를 탐지하는 것이 필요하며, 그 다음에는 어디에서 장애가 발생했는지 가능한 한 빨리 장애 위치를 파악하여 운영자에게 장애 정보를 통지하는 것이 필요하다. 본 시스템은 지능적인 관리를 통하여 보다 빠르고 정확한 장애 위치 확인 기능을 제공한다. <표 6>은 실시간 장애 탐지를 위한 기능들을 보여준다.

<표 6> 실시간 장애 탐지 기능

	기능	설명
실시간장애탐지기능	시스템 UP/DOWN 탐지	현재 시스템이 UP 인 상태인지 DOWN 인 상태인지를 판단하여 제공
	가동율(다운 횟수) 탐지	시간에 따른 가동률과 다운횟수를 계산, 제공
	Trap 기반 알람 통보	발생된 Trap 메시지를 수신하여 관리자에게 발생 시스템과 시간, 원인 등을 제공
	장애 로깅	다양한 형태로 발생된 장애를 로깅하여 제공

④ 네트워크 현황 분석보고 기능

네트워크의 가입 기관은 자신의 네트워크에 대한 현황과 자산 관리, 투자 지침 등의 보고서 정보를 보고 싶어한다. 본 시스템은 일간, 주간, 월간, 임의 기간 등을 기준으로 가입 기관의 상위 관리자에게 제공될 수 있는 종합적인 정보를 포함하는 총괄 보고서, 실제 네트워크 관리 실무자를 위한 상세한 분석 정보를 포함한 상세 보고서, 각 분석 항목을 기준으로 순위별로 정보를 제공하는 순위별 보고서 등을 제공한다. <표 8>은 네트워크 현황 분석보고를 위한 기능들을 보여준다.

<표 8> 네트워크 현황 분석보고 기능

	기능	설명
네트워크현황분석보고기능	기간 단위 보고서	특정 기간(일/주/월)에 따른 성능/장애 분석 정보 보고서 출력 기능
	그래프 형식 출력	다양한 그래프(표, 꺾은선, 파이)등을 통해 분석 정보 출력 기능
	관리자별 보고서	관리자 레벨에 따른 총괄, 상세 보고서 제공
	네트워크 자원 정보 보고서	지역 네트워크에 있는 네트워크 자원들에 대한 상세 정보를 기록하고 항목별 검색기능 제공

⑤ 고속 폴링 기능

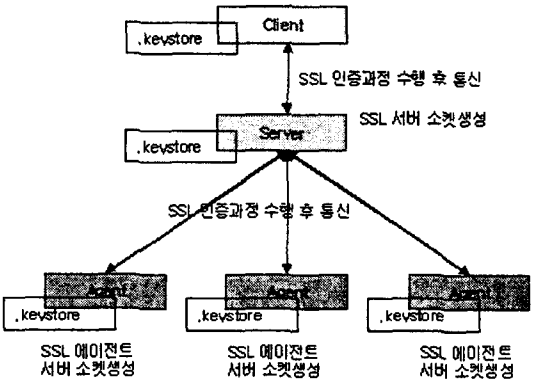
초고속 선로의 관리 정보를 수집하기 위해서는 보다 효과적인 폴링 기능을 제공해야 한다. 본 시스템에서는 관리 정보 수집을 위해 전문화되고 체계적인 알고리즘을 사용하여 효율을 증대 시킨다. 또한, *SNMPv2 MIB*과 초고속 선로를 위한 추가적인 MIB을 이용하여 풍부한 정보를 제공한다. 그리고, 별도의 DB를 통하여 관리 정보를 저장하여 많은 데이터를 고속 처리하는 기능을 제공한다. <표 9>는 고속 폴링을 위한 기능들을 보여준다.

<표 9> 고속 폴링 기능

	기능	설명
고속 폴링 기능	다중 폴링 기능	네트워크를 위하여 쓰레드 기반의 다중 폴링 기능 제공
	SNMPv2 MIB 또는 장비 추가 MIB 정보 제공	네트워크 관리를 위한 추가적인 MIB 또는 SNMPv2, SNMPv3 등의 사용
	시스템 폴링 간격의 동적 설정 기능	각 관리 대상별 차별된 폴링 간격을 설정하여 관리할 수 있도록 하는 기능
	관리 정보 요약 제공 기능	폴링한 관리 정보를 요약/압축하여 네트워크 센터 시스템에 전달해주는 기능

4.3 SSL을 이용한 통신 보안

앞에서 살펴보았듯이 기존에 네트워크 관리 시스템에는 많은 보안 취약요소를 안고 있다. 이런 보안 취약요소들을 해결하기 위한 많은 방법들이 있지만 여기에서는 SSL을 이용하여 기존에 네트워크 관리 시스템에 보안문제를 해결하고자 하였다. 네트워크 관리 시스템에서 SSL이 적용될 수 있는 부분은 크게 두 부분인데 첫째는 사용자 인터페이스를 제공하는 브라우저와 관리 서버간의 통신이고, 둘째는 관리 서버들간 통신에 SSL을 이용한 통신이 가능하다. (그림 6)은 클라이언트, 관리 서버, 보조 서버들의 SSL 통신을 위한 SSL 인증 절차를 보여주고 있다.



(그림 6) SSL 인증 절차

관리 서버들간이나 관리 서버와 사용자 인터페이스를 제공하는 클라이언트간에 SSL 인증과정을 살펴보면 다음과 같다.

i) 서버는 .keystore에 저장된 정보를 갖고 SSL 서버 소켓을 생성한다
ii) 클라이언트는 서버와 통신하기 위해 클라이언트 소켓을 생성하는데 이때 서버에 대한 정보를 .keystore로부터 얻어와서 SSL 클라이언트소켓을 생성하는데 사용한다.
iii) 클라이언트가 서버에 소켓 연결설정을 요구하면 서버에서는 인증에 필요한 정보를 요구하고 클라이언트가 이에 응답하므로 연결이 설정되게 된다.
iv) 연결 설정이 완료되면 서버와 클라이언트가 주고받는 데이터는 암호화하여 전송되고 수신 후에 복호화하여 사용하게 된다.

4.3.1 사용자와 관리 서버간의 통신

SSL은 웹 브라우저와 서버간의 통신을 암호화하는데 가장 많이 쓰인다. SSL을 지원하기 위해서는 우선 JSSE를 클라이언트에 설치하여야 한다. JSSE의 설치가 끝나고 필요한 설정을 마치

면 브라우저에서 SSL을 지원하는 서버와 통신할 수 있게 된다. 이를 위해서는 서버에도 JSSE를 설치하고 SSL 서버 소켓을 JSSE를 이용하여 생성하고 있어야 한다. SSL의 소켓은 javax.net.ssl.SSLServerSocketFactory로 만들게 된다. 그리고 accept()를 호출하면 들어오는 연결을 기다리게 된다. 연결이 들어오면 getInputStream()과 getOutputStream()을 호출하여 SSL 소켓 통신을 하는 것이다. (그림 7)과 (그림 8)은 각각 SSL 서버 소켓과 SSL 클라이언트 소켓을 생성하는 자바 코드를 보여주고 있다. 웹에서의 동적으로 페이지 구성을 위해 자바를 사용하여 구현하였다.

```
// allow a max of 10 sockets to queue up waiting for accept();
Security.addProvider(new com.sun.net.ssl.internal.ssl.Provider());
char[] passphrase = "isptest".toCharArray();
KeyStore keystore = KeyStore.getInstance("JKS");
keystore.load(new FileInputStream(".keystore"), passphrase);

// Now we initialize a KeyManagerFactory with the KeyStore
KeyManagerFactory kmf =
 KeyManagerFactory.getInstance("SunX509");
kmf.init(keystore, passphrase);

// Now we create an SSLContext and initialize it with
// KeyManagers from the KeyManagerFactory
SSLContext context =
SSLContext.getInstance("TLS");
KeyManager[] keyManagers =
 kmf.getKeyManagers();
context.init(keyManagers, null, null);

// First we need a SocketFactory that will create SSL server sockets.
SSLServerSocketFactory ssf =
context.getServerSocketFactory();
ss = ssf.createServerSocket(port, 10);
```

(그림 7) SSL 서버 소켓 자바 생성코드

```
// First we need to load a keystore
Security.addProvider(new com.sun.net.ssl.internal.ssl.Provider());
url = new URL(u, ".keystore");
Object obj = null;
DataInputStream datainputstream = new DataInputStream(new
BufferedInputStream(url.openStream()));

char[] passphrase = "isptest".toCharArray();
KeyStore keystore = KeyStore.getInstance("JKS");
keystore.load(datainputstream, passphrase);

// Now we initialize a TrustManagerFactory with the KeyStore
TrustManagerFactory tmf =
TrustManagerFactory.getInstance("SunX509");
tmf.init(keystore);

// Now we create an SSL Context and initialize it with
// TrustManagers from the TrustManagerFactory
SSLContext context = SSLContext.getInstance("TLS");
TrustManager[] trustManagers = tmf.getTrustManagers();

context.init(null, trustManagers, null);

// First we need a SocketFactory that will create SSL sockets.
SSLSocketFactory sf = context.getSocketFactory();

// Open a connection
sock = sf.createSocket(SERVER, PORT);
```

(그림 8) SSL 클라이언트 소켓 자바 생성코드

② 관리 서버들간의 통신

SSL이 사용되는 또 다른 부분은 관리 서버와 관리 서버간에 통신을 할 때이다. SSL을 사용하면 메시지 변조와 중간에서 훔쳐보는 행위를 막을 수 있다. 서버들간의 인증이 이루어져야 통신이 가능하므로 허가되지 않은 사용자가 서버에

메시지를 보내거나 요청할 수 없도록 하여 통신상에 정보를 보호해준다.

서버들간에 통신을 위해서는 우선 서버들 각자가 자신의 인증서를 만들고 SSL handshake 과정에서 서로 인증서를 교환하므로 서로를 인증하고 나면 둘 사이에 통신이 가능하게 된다. 서버들간에 통신에서는 서버 각각이 클라이언트와 서버의 기능을 수행하여야 하므로 통신을 위해서는 양쪽 모두 클라이언트 소켓과 서버 소켓을 생성하여야 한다. 생성 코드는 위에 (그림 7)과 (그림 8)에 나온 코드와 같은 코드를 사용한다.

5. 실험 및 고찰

5.1 구현 환경

5.1.1 서버(Server)

- Ultra SPARC 60: Solaris 7
- Jakarta-Tomcat 3.3: JSP 1.1, Servlet 2.2
- SSL v3.1(TLS v1.0)

5.1.2 클라이언트(Client)

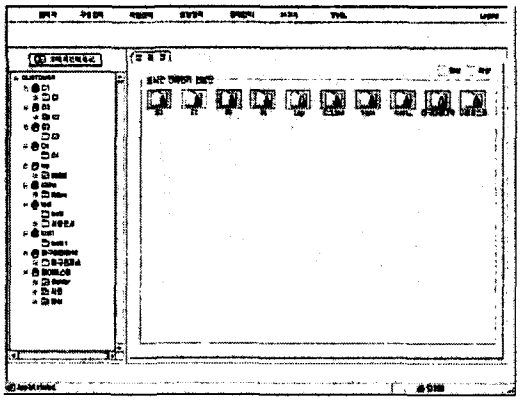
- Web-Browser: Internet Explore 5.5이상
- JDK 1.3, Javascript, Applet, HTML
- SSL v3.1(TLS v1.0)

5.1.3 데이터베이스

- Mysql 3.23

5.2 센터 관리 시스템

(그림 9)는 지역 네트워크나 소규모 네트워크의 상태를 나타내주는 상황판으로 등록된 장비들에 대한 장애 발생 여부를 실시간으로 리모터링 할 수 있는 가시화면을 제공해 준다. 장애가 발생한 지역 네트워크는 빨간 색으로 변하여 관리자가 쉽게 장애 여부를 파악할 수 있도록 해주고 이에 대한 제어를 할 수 있는 툴을 제공한다. 그리고 지역 네트워크 및 소그룹, 장비를 계층적인 트리 구조로 보여주므로 전체 네트워크 자원을 한눈에 파악할 수 있도록 해준다.



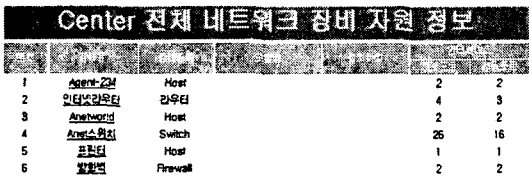
(그림 9) 센터 관리 시스템의 상황판

(그림 10)과 (그림 11)은 전체 지역 네트워크 및 소규모 네트워크의 자원정보, 장애현황, 성능분석 정보를 총괄적으로 보여주는 총괄보고서와 성능 분석항목에 따른 순위별 분석을 보여주는 성능분석, 장애 항목에 따른 특정 기간동안의 누적분석을 보여주는 장애현황, 그리고 장애 항목의 순위별 분석결과를 보여주는 장애 순위별 보고서를 보여준다.

3.성능분석

자연관-1	166.104.100.13_3001	0.16	0.32	0.00
자연관-1	166.104.100.13_3002	0.13	0.01	0.00
자연관-1	166.104.100.13_4001	0.13	0.19	0.00
자연관-1	166.104.100.13_4002	0.25	0.19	0.00
자연관-1	166.104.100.13_4003	0.41	0.09	0.00
자연관-1	166.104.100.13_4004	0.04	0.13	0.00
자연관-1	166.104.100.13_4005	0.01	0.09	0.00
자연관-1	166.104.100.13_4006	0.02	0.06	0.00
자연관-1	166.104.100.13_4007	0.09	0.04	0.00
자연관-1	166.104.100.13_4008	0.02	0.09	0.00
기숙사	166.104.100.19_3001	0.03	0.00	0.00
기숙사	166.104.100.19_3002	0.01	0.00	0.00
외학정보-1	166.104.104.14_3001	0.04	0.00	0.00
외학정보-1	166.104.104.14_3002	0.00	0.00	0.00
학술-1	166.104.192.13_2001	0.01	18.12	0.00
학술-1	166.104.192.13_3	0.00	0.00	0.00

(그림 10) 성능 보고서


Center 전체 네트워크 장비 자원 정보

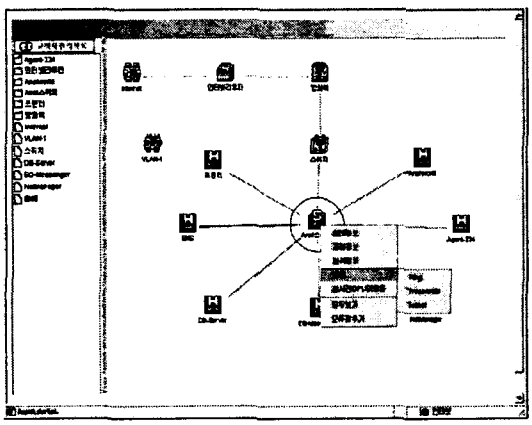
1	Agent-2H	Host	2	2
2	인터넷라우터	라우터	4	3
3	Anetworld	Host	2	2
4	Anet스위치	Switch	26	16
5	프린터	Host	1	1
6	방화벽	Firewall	2	2

(그림 11) 총괄 자원정보

센터 관리 시스템에서는 주로 전체 네트워크에 대한 상태 정보를 제공하고 지역 네트워크에 장애가 발생하였을 때 지역 네트워크로부터 보내온 트랩 정보들을 받아 처리하므로 원활한 네트워크 관리를 수행하도록 하고 있다. 그리고 지역 관리 시스템으로 접근할 수 있는 인터페이스를 사용자에게 제공하면 전체 네트워크 자원들에 대한 총괄적이고 통계적인 정보를 제공한다.

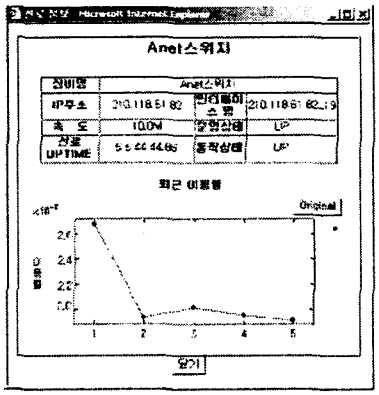
5.3 지역 관리 시스템

(그림 12)는 지역 네트워크의 실시간 네트워크 상태를 보여주는 상황판이다. 화면은 네트워크 장비와 이것을 연결하는 선로로 구성되어 있으며, 네트워크의 상황에 따라 장비 UP/DOWN, 선로 트래픽 레벨 등이 구분되어 표시된다. 그리고 실시간 이용률과 에러율 정보를 제공한다.



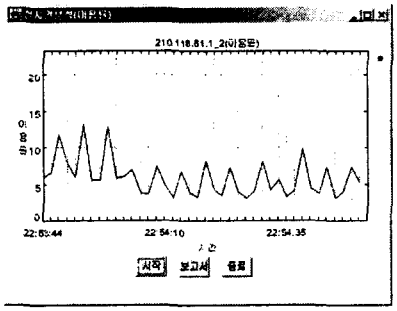
(그림 12) 지역 관리 시스템의 상황판

(그림 12)는 회선의 누적정보를 보여주고 있다. 네트워크 관리를 위해서는 실시간 성능 정보가 필요하지만 이들 정보를 DB에 저장하여 네트워크의 현재뿐만 아니라 과거의 상태 및 성능을 파악할 수 있도록 누적정보를 제공하고 있다.



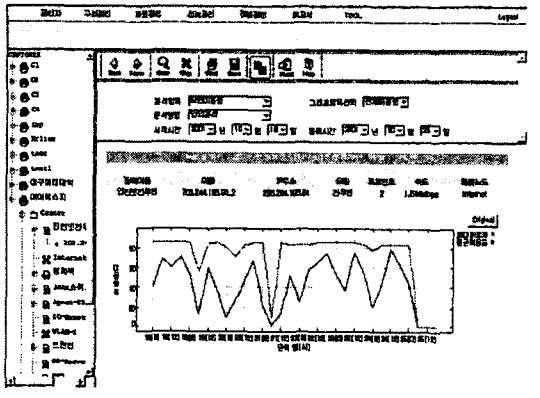
(그림 12) 회선의 누적정보

(그림 13)은 지역 관리 시스템의 상황판에서 특정 장비를 선택하여 이 장비의 이용률에 대한 실시간 정보를 보자고 할 때 나타나는 프레임으로 몇 초당위로 폴링하여 정보를 보여준다.



(그림 13) 회선의 실시간 이용률

(그림 14)는 지역 네트워크에 속해있는 자원들에 대한 성능 정보를 보여주는 것으로 지역 네트워크에 대한 전체적인 성능 평가를 할 수 있는 정보를 제공한다.



(그림 14) 성능 관리

6. 결 론

인터넷을 통해 온라인 계좌이체나 신용 카드 결제 등의 온라인 결제를 할 때 가끔 자신의 정보가 유출되어 불이익을 보는 경우를 보게 되는데 이와 같은 문제가 발생하는 이유는 네트워크 보안을 고려하지 않고 네트워크를 구축하였기 때문에 악의를 가진 제3자가 공유회선을 따라 흘러 다니는 정보를 훔쳐 볼 수 있기 때문이다. 이렇게 습득한 정보를 제3자가 자신의 이익을 위해 악의적으로 사용한다면 정보를 유출한 당사자는 큰 피해를 입을 수도 있게 된다. 이런 문제는 보안이 약한 네트워크 관리 시스템도 발생할 수 있다. 네트워크 관리 시스템들이 로컬 네트워크 관리를 위해서만 사용된다면 위의 보안문제들은 크게 걱정하지 않아도 된다. 하지만 지역적으로 떨어진 대규모의 네트워크를 통합적으로 관리하려고 하거나 MSP 사업자들이 산재해 있는 네트워크를 관리하기 위해서는 이들 네트워크 관리 시스템이 로컬 네트워크가 아닌 다른 네트워크에 있는 장비들로부터 정보를 주고받게 된다. 이때 통신 회선은 여러 사용자가 같이 사용하는 공유 회선을 사용하므로 네트워크에 흐르는 정보들을 제3자가 훔쳐보는 것이 가능하다. 이런 경우 유출된 정보로 인하여 네트워크 일부 또는 전체에 영향을 미칠 수 있다.

네트워크 장비들은 각각이 네트워크에서 중요한 역할을 수행하고 있다. 이들 장비가 정상적으로 동작하지 않으므로 인해 네트워크 일부 또는 전체가 동작하지 않을 수도 있다. 그렇기 때문에 관리 정보의 유출로 인해 발생할 수 있는 문제를 미연에 예방하기 위하여 통신 보안이 필요하다.

이에 본 논문에서는 기존에 네트워크 관리 시스템에서 관리 서버와의 통신이나 클라이언트와의 통신에 외부로부터의 침임을 막기 위하여 SSL을 이용한 네트워크 관리 시스템을 설계 및 구현하였다. 하지만 SSL을 이용하므로 서버간이나 클라이언트와의 통신상에 문제는 해결하였지만 SSL을 이용한 통신을 위해서 필요한 인증서나 비밀키에 대한 관리문제도 생겨나게 되었는데 이런 문제점들에 대한 보안책도 연구되어야 할 것이다.

참고문헌

[1] H. J. Kang, J. W. Kim, S. J. Ahn, J. W. Chung, "A Circular Management Data Gathering Protocol for Efficient Network Management System", The 9th International Conference on Information Networking, 1994.

[2] 안성진, 정진욱, "SNMP MIB-II를 이용한 인터네트 분석 파라미터 계산 알고리즘에 관한 연구", 정보처리학회, Vol.2, No.2, 1998

[3] 유승근, 안성진, 정진욱, "SNMP MIB-II를 이용한 인터넷 관리 시스템의 웹 인터페이스 설계 및 구현", 정보처리학회논문지, Vol.6, N.3, pp421-430, 2002

[4] 이원혁, 안성진, 정진욱, "계층적 관리 구조

를 갖는 정보 자원 관리 시스템의 설계 및 구현", 정보처리학회논문지, Vol.9, N.3, pp699-709, 1999

[5] William Stallings, "SNMP, SNMPv2, and CMIP : the practical guide to network management standards", Addison-Wesley Publishing Company, 1993

[6] William Stallings, "SNMP, SNMP v2, and RMON Practical Network Management", Addison-Wesley Publishing Company, 1996

[7] J. H. Koo, "A Study on the Design of Web-based Interface for Network Traffic Analysis System" The Graduate School of Sung Kyun Kwan University, 1997

[8] Jonathan Knudsen, "Java Cryptography", O' reilly, 1999

[9] Jess Daniel, "Java Security", Wrox, 2001

[10] Gilbert Held, "LAN Management with SNMP and RMON", Wiley Computer Publishing, 1996

[11] Gary Cornell, Cay S. Horstmann, "Core JAVA", Prentice Hall, 1996

[12] Elliotte Rust Harold, "Java Network Programming", O' reilly, 1997

황 일 선

1996년 시스템공학연구소(SERI) 실장
1998년 한국전자통신연구원(ETRI) 초고속정보망 실장
1998년 ~ 현재 한국과학기술정보연구원(KISTI) 슈퍼컴퓨팅센터 초고속연구망 실장

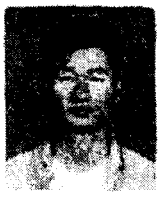
이 명 선

1991년 한남대학교 전자계산학과(학사)
2002년 성균관대학교 전기전자공학과 정보공학전공 박사과정
2002년 ~ 현재 한국과학기술정보연구원 선임연구원

유 기 성

1983년 아주대학교 전자공학과(학사)
1996년 한남대학교 컴퓨터공학과(석사)
1983년 ~ 현재 한국과학기술정보연구원 책임연구원
1997년 ~ 현재 한남대학교 컴퓨터공학과 박사과정

김 종 근



2001년 성균관대학교 전기전자 및 컴퓨터공학부(학사)
2001년 ~ 현재 성균관대학교 정보통신공학부 석사과정

조 강 홍

1997년 성균관대학교 정보공학과(학사)
1999년 성균관대학교 전기전자 및 컴퓨터공학부(석사)
1999년 ~ 현재 성균관대학교 정보통신공학부 박사과정

정 진 욱

1974년 성균관대학교 전기공학과(학사)
1979년 성균관대학교 전자공학과(석사)
1991년 서울대학교 계산통계학과(박사)
1982년 ~ 1985년 한국과학기술 연구소 실장
1981년 ~ 1982년 Racal Mil해 Com. 객원연구원
1991년 ~ 현재 성균관대학교 정보통신공학부 교수