IP 통합 관리를 통한 유·무선 네트워크의 생존성 향상에 관한 연구

김 시 흥* · 구 자 환* · 박 병 연** · 박 학 수** · 최 장 원** · 이 재 용***

요 약

컴퓨터 네트워크는 산업 전반에 응용되고 대중화되어 급속하게 우리의 삶에 파고들고 있다. 이와 더불어 네트워크에 대한 침해도 지능적화, 다양화되어 이에 대한 해결책이 시급한 실정이며 사전에 방지 하기보다는 다양한 네트워크 공격을 받더라도 서비스를 계속할 수 있는 네트워크의 생존성에 관한 사항이 주목을 받고 있다. 이에 본 논문에서는 네트워크의 생존성을 향상시키는 방안으로 IP 통합 관리를 이용하는 방안을 제안하였으며 유·무선 환경에 적용하기 위하여 유·무선 보안 기술을 응용한다. 네트워크의 패킷 모니터링을 통하여 IP/MAC 주소 관리함으로써 관리 네트워크내의 임의의 사용자가 사용중인 네트워크 장비 혹은 PC의 IP 주소나 네트워크 인터페이스 카드를 임의적으로 또는 악의적으로 변경하는 것을 차단할 수 있고 웜과 같은 부적절한 네트워크 현상을 발견하여 시스템을 차단하는 방안을 제시한다.

A Study on the Improvement of Wired and Wireless Network Survivability using Integrated IP Management

Si-hung Kim* · Ja-Hwan Koo* · Byung-Yeon Park**
Hark-Soo Park** · Jang-Won Choi** · Jae Young Lee***

ABSTRACT

Computer Communications and networks have been revolutionized by technological advances in the last decade. There has been an increasing interest in the network security because of the growing popularity of Internet and the importance of networking in business area. With this growing interest, Network engineers come to more concern about improving network survivability. In this paper, we suggest the method that improves the survivability of wired and wireless network. To achieve this goal, we propose the integrated IP management with monitoring network nodes in the same network and controlling its activities.

* 성균관대학교 정보통신공학부
** 한국과학기술정보연구원
** 한서대학교 인터넷 공학과

1. 서 론

오늘날 컴퓨터와 통신 기술의 발전은 초고속 네트워크 인프라 구축을 가능하게 했을 뿐만 아니라 정부 기관을 비롯한 금융권, 기업체, 개인에 이르기까지 각종 정보를 공유하게 함으로써 사회 전반에 큰 변화를 가져오게 하였다. 유선네트워크는 가정이나 사무실에서 모뎀이나 LAN으로 접속하는 환경으로 변화하였으며 이동통신은 전 국민의 절반 이상이 단말기를 소지할 정도로 급격하게 확산되었다. 무선 인터넷은 이러한 두 개의 거대한 축의 통합 과정을 통해 탄생하였다. 무선 인터넷은 인터넷이라는 네트워크의 탈 중심적, 개방적, 양방향성 등의 특성과 이동통신의 이동성, 양방향성, 개인화의 특성을 그대로 물려받고 있다. 즉 무선 인터넷은 사용자가 이동 중 무선 네트워크를 통해 인터넷 서비스를 제공받을 수 있는 환경과 기술을 말한다. 무선 인터넷을 이용하면 이동전화나 PDA 등의 이동통신 단말기로 언제 어디서나 인터넷에 접속할 수 있으므로 다양한 정보 검색과 전자상거래 등을 이동통신 단말기를 이용해서 수행함으로써 기존의 인터넷 환경의 시간, 공간적인 제약을 극복할 수 있게 된다.

그러나 이와 더불어 컴퓨터 네트워크를 통해 정보가 위조 또는 변조되고, 중요한 정보가 허락없이 유출되는 등 각종 불법 행위가 빈번하게 발생함으로써 정보화 발전으로 인해 발생하는 역기능의 폐해가 점점 증가하고 있다. 무선 인터넷 또한 예외일 수 없어 이러한 문제는 앞으로의 무선 인터넷 시대로의 하나의 큰 걸림돌이 될 것이며, 이에 대한 조기의 대처가 필요한 실정이다.

이 같은 위험을 사전에 방지하고 유·무선의 인터넷상에서 안전한 정보 공유와 작업을 가능하도록 하기 위해서 대부분의 기관이나 기업들은 네트워크 보안 대책 방안으로 방화벽, 침입탐지 시스템, 가상 사설망 등과 같은 보안 제품을 설치하고, 네트워크 보안 담당자를 두어 운영하고 있다. 그러나 이러한 구성만으로 유동적인 네트워크 보안에 대한 완전한 안전성이 보장되는 것은 아니며, 네트워크에서 취약한 여러 요인들의 제거를 위해서는 다양한 유·무선 인터넷 통합 솔루션들을 보안 정책에 따라 총괄적이며 체계적으로 설치, 운영할 수 있는 인프라의 구축이 필수적이다.[1] 이에 본 논문에서는 유·무선 인터넷에서 통합적인 IP 주소 관리를 통해 네트워크의 통제와 동적으로 생존성을 확보하는 문제는 유·무선 통합 환경에서의 솔루션 개발에 획기적인 방안이며, 본 논문에서 이에 대한 방안을 제시하고자 한다.

본 논문에서는 IP 주소 통합 관리를 통한 유·무선 네트워크의 생존성을 보장하는 방안을 제시한다. 먼저 2장에서는 네트워크 생존성에 관한 전반적인 사항을 다루고, 3장에서는 유·무선 환경에서 IP 통합 관리를 위해 보안적 서비스를 제공할 수 있는 기술들을 살펴본다. 4장에서는 IP 주소 통합 관리 방안의 흐름에 대해 논하고자 한다.

2. 네트워크 생존성 향상

2.1 네트워크 생존성

네트워크에 대한 공격이 다양화되고 치밀해 지고 있는 가운데 이를 막기 위한 네트워크 보안 기술도 다각도로 연구가 되어지고 있다. 현재 네트워크 보안 기술은 침입 징후를 탐지하기 위한 침입 탐지 시스템과 탐지된 해당 침입자의 트랙픽의 차단을 주 목적으로 하는 방화벽이나 패킷 필터링 라우터와 같이 자신의 도메인을 보호하기 위한 대응 시스템, 그리고 네트워크의 생존성을 높이는 시스템 등이 있다[9]. 네트워크 생존성이란, 네트워크에 침해 공격이나 시스템 결함, 과다한 부하 등으로 시스템에 피해가 발생하더라도 지속적으로 동작하여 서비스를 제공하는 것

을 말한다. 초기의 보안은 공격에 대한 방어 기술을 단일 컴퓨터 상에서 연구하는 형태로 진행되었지만, 현재는 네트워크 공격에 대처하는 기술과 이를 견디어 내는 기술이 개발되고 있다. 즉, 네트워크를 구성하는 구성요소와 구성된 네트워크의 유기적인 조직 관리를 통한 보안관리에 네트워크 생존성의 초점이 맞춰지고 있다[7, 8].

2.2 네트워크 생존성 방안

네트워크 생존성에 관한 연구는 DARPA를 중심으로 활발히 진행 중에 있으며 ITS(Intrusion Tolerant System), FTN(Fault Tolerant Network), DC(Dynamic Coalitions)의 개념으로 나누어 세부적인 틀을 형성하고 있다.

ITS는 시스템에 외부 공격자에 의해 침해가 시도되어 피해가 발생하거나 시스템 내부의 결함으로 피해가 발생하여도 사용자에게 정확한 정보로 서비스를 지속적으로 제공하는 정보 시스템을 말한다. 기존의 정보보호 연구에서 진행되었던, 방어 메커니즘인 방화벽, 침입 탐지 시스템 등을 성공적으로 회피하여 침투한 공격으로 인해 발생하는 시스템의 피해를 탐지할 수 있어야 하고, 탐지한 피해의 특성을 파악하여 필수 서비스를 지속적으로 제공하기 위한 대응방법을 적용할 수 있어야 한다. 외부 공격이나 내부 결함으로 인해 정보 시스템에 발생한 피해에 대한 대응 방법으로는 대부분 하드웨어의 재구성이나 소프트웨어적 자원 재 할당 방법 등을 적용한다. 즉, 침입 감내 시스템은 시스템에 외부 공격자에 의한 침입과 시스템 내부에서 발생하는 결함으로 인해 피해가 발생하더라도 필수 서비스를 제공할 수 있는 기술을 개발하는 것을 목표로 하고, 이러한 목표를 수행하기 위해 시스템에 서비스를 제공하는데 필요한 자원들을 중복하여 관리하고, 피해가 발생하더라도 중복된 자원들의 대체를 통해 서비스의 중단을 방지하는 기술과 하드웨어적인 구성을 변경하여 지속적인 서비스를 제공하는 기술을 개발한다. ITS가 정보 시스템으로 시스템의 침입과 결함으로 피해가 발생하고 있더라도 사용자에게 정보를 지속적으로 제공하기 위한 연구라고 한다면, FTN은 네트워크 차원의 노드 중복성을 이용하여 사용자에게 가용성을 보장하기 위한 연구라 할 수 있다. FTN은 네트워크가 공격을 받고 있고, 공격 성공으로 인해 피해가 발생하더라도 네트워크에서 제공하는 기능과 서비스는 지속적으로 사용자에게 제공하는 방안을 연구한다. 즉, 공격 성공으로 인해서 발생하는 네트워크의 피해를 최소화하고, 네트워크 사용자를 효율적으로 관리하여 인가된 사용자에게 서비스를 제공하기 위한 최소한의 네트워크 기능은 지속적으로 유지하여 네트워크의 가용성을 보장하려는 연구이다. 이러한 목적을 위하여 서비스 거부 공격을 방어하고 관리할 수 있는 기술과 공격자의 근원지를 찾아내는 기술, 공격자에 의해서 입은 피해를 복구하고 네트워크의 기능을 정상화시키는 기술 등에 대한 연구가 진행하고 있다.

DC는 네트워크의 필수 기능을 제공하기 위해, 서로 다른 네트워크들의 연합을 구성하여 각 네트워크에 분산 적용된 보안 정책과 메커니즘을 동적으로 통합 관리하여 사용자에게 지속적인 서비스를 제공하려는 연구이다.

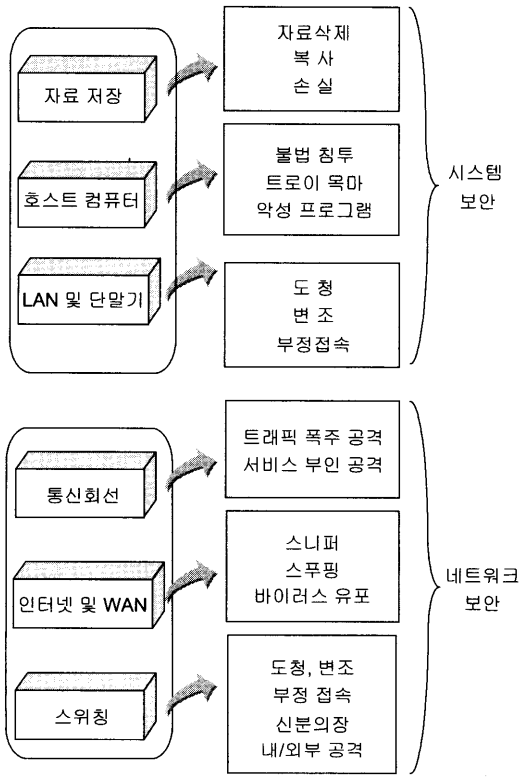
3. 유·무선 보안 기술

3.1 보안 기술의 개요

최근 들어 해킹, 바이러스 등의 보안사고 발생 사례가 급증하면서 일반인들의 보안 기술에 대한 관심도 증가하고 있다. 특히 인터넷을 통해서 쇼핑, 증권, 금융 업무 등 경제 문제와 직결되는 서비스의 제공이 늘어나면서 보안 기술의 중요성은 더욱 강조되고 있다.

일반적으로 정보통신 시스템에 대한 위협 요소는 (그림 1)과 같이 분류할 수 있는데 이에 대응

하는 보안 기술은 크게 2가지로 구분할 수 있다.



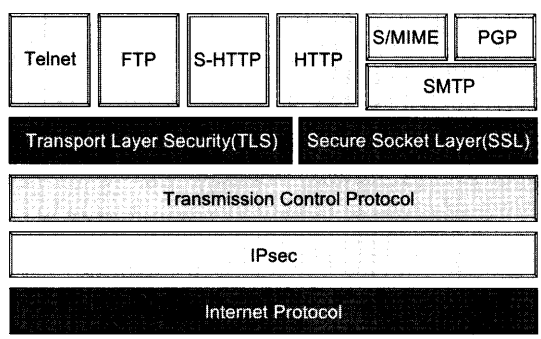
(그림 1) 보안위협 요소의 분류

첫째는 시스템 보안이며, 다른 하나는 네트워크 보안이다. (그림 1)에서 호스트 컴퓨터나 단말기에 대한 불법 침투, 부정 접속, 신분 위장, 자료 삭제 및 손실 등의 공격에 대한 방어는 시스템 보안에 속한다. 즉 시스템 보안은 해킹, 바이러스와 같은 공격에 대해서 정보보호 서비스를 제공하며, 주로 운영체제 보안과 관련이 있다. 또한 시스템 보안의 하나로 최근 많은 관심을 끌고 있는 침입 탐지 시스템이 있다. 침입 탐지 시스템은 시스템이 네트워크에 대한 침입을 즉각적으로 탐지하고 대처할 수 있는 기술로 침입자에 대한 불법적인 사용을 탐지하고, 합법적인 사용자에 의한 오용이나 남용을 탐지하는 것이 목표이다. 시스템 보안에 대한 연구는 비교적 역사가 깊으며 다수의 시스템 보안 도구가 개발되어 있고, 정보보호 시스템에 대한 평가 기준 및 평가제도 또한 잘 정비되어 있다.

인터넷이 보편화되고 네트워크의 규모가 커짐에 따라 보다 강조되고 있는 네트워크 보안은 네트워크상에서의 도청, 메시지 변조, 신분 위장 등의 공격에 대해서 정보보호 서비스를 제공한다. 네트워크 보안을 통해 제공되는 정보보호 서비스는 크게 다음과 같은 4가지가 있다.

- 기밀성 : 네트워크를 통해 전송되는 데이터는 권한이 부여된 사람만이 내용을 볼 수 있어야 한다.
- 사용자 인증 : 메시지를 작성한 사람의 신원을 확인할 수 있어야 한다.
- 데이터 무결성 : 전송된 데이터가 전송 도중에 변경되었는지 확인할 수 있어야 한다.
- 부인 봉쇄 : 송신자가 메시지를 송신한 사실을 부인하거나 수신자가 메시지 수신 사실을 부인할 수 없어야 한다.

이러한 정보보호 서비스는 하나의 메커니즘을 통해서 모두 제공될 수 없으며, 여러 가지 다양한 메커니즘에 의해서 제공되는 것이 일반적이다. (그림 2)는 인터넷의 기반인 TCP/IP에서 대표적인 네트워크 보안 메커니즘을 보여준다.



(그림 2) 네트워크 보안 메커니즘

IPsec은 IP 계층에서 정보보호 서비스를 제공하며, TLS/SSL은 TCP 계층과 애플리케이션 계층 사이에 위치한다. S/MINE과 PGP는 이메일 보안 도구이며 S-HTTP는 애플리케이션 계층인 HTTP에 보안 서비스를 제공한다. 이밖에도 대표적인 네트워크 보안 메커니즘으로 침입 차단 시스템을 들 수 있다.

3.2 유·무선 PKI 응용

IP 통합 대상으로부터의 메시지 인증이나 데이터의 전송은 PKI 기술을 응용한다. 유선 네트워크 환경과 마찬가지로 무선 네트워크에 대해 안전한 서비스를 제공하기 위해서는 기밀성, 무결성, 인증, 부인봉쇄와 같은 보안 서비스를 제공하기 위한 무선 PKI 기술이 필요하다. 무선 PKI란 기존의 유선 PKI의 구성요소를 그대로 이용하며, 무선 환경에 적합하도록 기능을 최소한 변화시킨 것이다. 무선 PKI의 구성 요소는 다음과 같다.

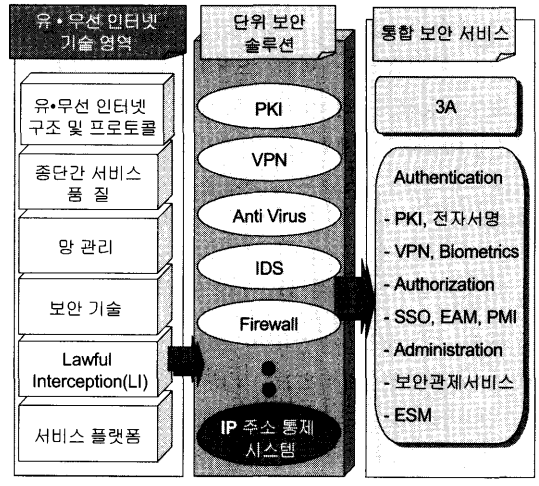
1) 인증기관 : 인증서를 발행하고 효력정지 및 폐지 기능을 수행한다.
2) 등록기관 : 인증서 등록 및 사용자 신원 확인을 대행한다.
3) 디렉토리 : 인증서 및 인증서 폐지목록을 저장한다.
4) 사용자 : 인증서를 신청하고 인증서를 사용한다.

위에서 설명한 무선 PKI를 구성하는 4개의 중추적인 구성요소 외에 무선 인터넷 사용자를 대신하여 인증서 상태 정보와 함께 인증 경로에 대한 검증 정보들을 제공하는 OCSP(Online Certificate Status Protocol)나, 무선 단말기의 계산 능력 저하로 인한 단점을 보완하기 위하여 사용되는 보안 모듈 등이 무선 네트워크 상에서 PKI를 구성하기 위한 부수적인 구성 요소이다.

4. 유·무선 네트워크에서의 IP 통합 관리 기술

4.1 IP 통합 관리의 개념

IP 주소 통제 및 관리란 네트워크 내의 패킷을 실시간으로 모니터링 함으로써 관리 네트워크내의 임의의 사용자가 사용 중인 네트워크 장비 혹은 PC의 IP 주소나 네트워크 인터페이스 카드를 임의적으로 또는 악의적으로 변경하거나 또는 웜이나 기타 이상행동을 포착하여 단말 시스템의 기능을 차단함으로써 네트워크의 생존성을 보장하는 것을 말한다. 또한 새로운 네트워크 지원 장비의 도입 시 수많은 네트워크 자원을 임의적으로 할당하지 않고, 관리자가 관리하게 됨으로써 효율적인 자원관리 및 네트워크 문제 발생 시 신속한 대처를 할 수 있다. 이것은 하위 레벨에서의 네트워크 관리 및 보안을 유지할 수 있게 한다.



(그림 3) 유·무선 네트워크의 IP 통제 시스템

최근의 세계적 추세를 보면 대부분의 통신 사업자는 기존 교환기 중심의 유선 전화망을 패킷 기반 네트워크로 전환시켜 나가고 있고, 무선 인

터넷의 경우에도 ALL IP 개념이 도입되어 음성, 데이터, 영상이 통합되는 멀티미디어형 서비스 제공에 박차를 가하고 있다. 더불어 차세대 무선 인터넷을 실현하기 위해 세부 요소 기술에 대한 표준화 작업들이 다방면에서 이루어지고 있다. 이로써 IP의 통합 관리와 IP의 차단은 네트워크를 관리할 수 있다는 근거를 가지게 되며 새로운 개념의 보안 솔류션으로 생각해 볼 수 있다. (그림 3)는 IP 주소 통제 시스템의 보안 솔루션으로써의 위치를 보여 주고 있다.

4.2 IP 통합 관리 구성

IP 통합 관리는 네트워크에서 사용되는 IP 주소와 이를 제어하는 메니저 시스템과 메니저에게 정보를 제공하기 위해 네트워크를 모니터링하는 에이전트로 구성된다. 메니저는 에이전트 시스템으로부터 수집된 IP 주소 및 네트워크 자원 정보를 받아들여 네트워크의 정확한 현황을 파악하며 이를 토대로 설정된 정책에 위배되는 사항을 검출한다. 정책은 네트워크의 특성에 맞게 관리자가 메니저 시스템의 조작을 통해 설정할 수 있으며, 정책에 위배되는 트래픽 발견 시 단말 시스템에 대한 제한을 에이전트에게 명령하게 된다. 메니저는 아래와 같은 세부 기능으로 구성된다.

4.2.1 중앙 집중적 IP 주소 관리 기능

관리 시스템은 분산되어 있는 에이전트 시스템들이 수집한 네트워크 정보 및 IP 주소를 수신 받는다. 이런 정보를 중앙에서 관리함으로써 IP 주소의 중복 사용을 피할 수 있고, 전체적인 IP 주소 사용 내역에 대한 통계를 낼 수 있다.

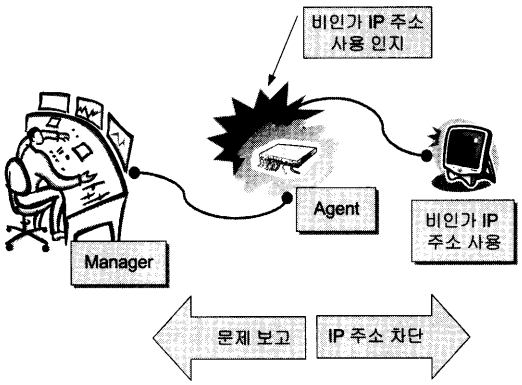
4.2.2 IP 주소 사용 인증 관리 기능

관리자는 현재 사용중인 IP 주소를 관리 정책과 비교하여 정책에 위반되거나 비 인가된 사용자에 대해서는 IP 주소를 차단시킴으로써 네트워크 사용을 불가능하게 만들고 보안을 강화할 수 있다.

에이전트 시스템은 네트워크 세그먼트마다 설치되어 네트워크의 자원 정보 및 IP 주소를 수집하여 관리 시스템에게 통보하고 관리 시스템의 정책에 따라 IP 주소를 제어하는 시스템이다. 중앙 집중적인 관리 방식은 트래픽의 과부하를 발생시키기 때문에 분산적인 네트워크 환경에서는 에이전트 개념을 적용시킨다. 에이전트는 아래와 같은 세부 기능으로 구성된다.

1) 네트워크 자원 정보 자동 수집 기능
   네트워크에 연결된 모든 자원인 IP 주소, MAC 주소, 시스템 이름, 사용자 이름을 자동으로 수집하는 기능이다. 수집된 정보는 관리 시스템에게 전달하고, 관리 시스템은 이 정보를 토대로 현재 사용중인 IP 주소 현황을 파악하고, 필요에 따라 IP 차단과 같은 제어 기능을 수행할 수 있다.
2) IP 주소 실시간 모니터링 기능
   현재 네트워크에서의 브로드캐스트 패킷만을 실시간으로 모니터링 함으로써 네트워크 장비의 변경 없이 네트워크 IP 주소 관리가 가능하다.
3) 단말 시스템 차단 기능
   관리 시스템으로부터 인가된 IP 주소 목록을 전달받아 현재 네트워크에서 실시간 모니터링 기능으로 수집한 IP 주소를 비교하여 비인가된 IP 주소가 사용중이면 이 단말 시스템을 차단함으로써 네트워크 통신을 불가능하게 하고 보안 기능을 강화시킬 수 있다.

(그림 4)는 정책에 맞지 않는 네트워크 자원 사용 즉 비인가 IP 사용을 발견했을 시에 메니저와 에이전트 시스템간의 메시지 교환을 나타내고 있다.



(그림 4) IP 관리 및 차단의 흐름

5. 결 론

본 논문은 유·무선 네트워크 환경에서 네트워크 생존성을 보장하는 방안으로 IP 통합 관리를 이용하는 방법에 관한 것이다. IP/MAC 주소의 통합 관리에 초점을 맞추어 네트워크의 생존성을 향상시키고 IP 주소의 임의적 변경 또는 악의적 사용에 의한 각종 장애에 대처할 수 있는 기능을 제공함으로써 네트워크 보안의 기능을 함과 동시에 네트워크의 장애에도 대처할 수 있는 방안을 제시하였다. 향후 더 나은 네트워크 보안을 위해 다른 보안 솔루션(예를 들어 방화벽이나 VPN)과의 접목 기술이 요구되며 이때 고속으로 패킷을 처리할 수 있는 방안이 필요할 것이다.

참 고 문 헌

[1] Jain, S., Shenoy Ramam, D., Thirumalasetty, S. R., Saddi, M., Summa, F., "A network management framework for multi-layered network an overview", Integrated Network Management Proceedings, 2001 IEEE/IFIP International Symposium on, pp.14-18, May 2001.

[2] M. A. Hasan, "Power Analysis Attacks And Algorithmic Approaches To Their Countermeasures For Koblitz Curve Crypto-system", 1988.

[3] R. Diaz-Caldera, "An Approach to the Cooperative Management of Multitechnology Networks", IEEE Comm. Mag., Vol.37, No.5, pp.119-125, May 1999.

[4] P. Demeester et. al., "Resilience in Multilayer Networks", IEEE Comm. Mag., Vol.37, No.8, pp.70-76, August 1999.

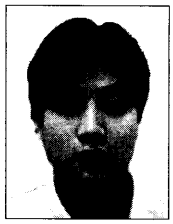
[5] D. Medhi, "A Unified Approach to Network Survivability for Teletraffic Networks : Models, Algorithms and Analysis", IEEE Trans. Comm., Vol.42, pp.534-548, 1994.

[6] D. Medhi, S. Jain, D. S. Ramam, S. R. Thirumalasetty, M. Saddi, F. Summa, "Network Management for Multi-Layered Network Survivability : Management Framework and Implementation", CST Technical Report, University of Missouri-Kansas City, 2000.

[7] W. G. Bliss and L. L. Scharf, "Algorithms and Architectures for Dynamic Programming on Makov Chains", IEEE Trans, ASP 37, pp.900-912, 1989.

[8] Y. K. Agarwal, "An Algorithm for Designing Survivable Networks", AT&T Technical Journal, Vol.58, No.3, pp,64-76, 1989.

[9] T. Jackson, M. Wlikens, "Survivability of Networked Information Systems and Infrastructures : First Deliverable of an explanatory study", European Commission Special Report JRC/ISIS/STA/DAS/Projects/Survivability/Study, pp.1-37, Dec. 1998.

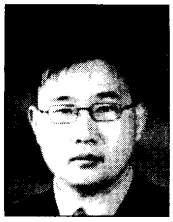


김 시 흥

성균관대학교 정보통신공학부
(공학사)
성균관대학교 정보통신공학부
석사과정

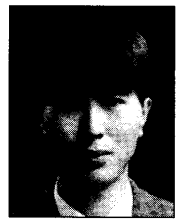
구 자 환

성균관대학교 정보공학과
(공학사)
성균관대학교 정보공학과
(공학석사)
현재 성균관대학교 정보통신공
학부 박사과정
LG CNS 정보기술연구소 연구원



박 병 연

대전산업대학교
공주대학교 교육정보대학원
KIST/시스템공학연구소 입사
한국전자통신연구원
한국과학기술정보연구원



박 학 수

한남대학교 공학박사
KIST/시스템공학연구소 입사
연구개발정보센터
한국과학기술정보연구원

최 장 원

홍익대학교 공학석사
현재 고려대 박사과정
연구개발정보센터 입사
한국과학기술정보연구원

이 재 용

인하대학교 공학학사
인하대학교 공학석사
인하대학교 공학박사
유한대학 강사
재능대학 강사
시스템 공학 연구소 연구원
수원여자대학교 조교수
한서대학교 조교수