通信情報保護學會誌
第3卷 第1號, 1993. 3

무선 데이타 통신망을 위한 무선채널 Security

임병렬* · 나종근** · 김동규***

1. 서 론

정보통신 기술의 발달은 지원의 공유 및 정보의 전송에 있어 사용자의 다양한 요구사항을 충족시킬 수 있을 뿐만 아니라 이를 바탕으로한 네트워크 기술의 발달로 통신 환경은 광역화되어 원격한 통신 당사자간에도 자유로운 통신을 보장하게 되었다. 더우기, 현대 사회가 정보의 신속한 교환이 요구되는 정보화 사회로 나아감에 따라 특정 장소의 제약을 극복하기 위한 이동통신 및 무선 데이타통신이 대두하게 되었다. 국내의 이동통신은 해마다 폭발적인 증가를 하고 있으며, 앞으로의 몇년간은 이러한 양상이 계속될 것이다. 그러나, 무선 데이타통신 분야에 대한 국외의 동향은 개인용 컴퓨터의 소형화 추세에 따른 단말기에 이동성 부여로 무선 네트워크를 이용하고자 하는 수요 및 서비스가 급격히 증가하는데 반해 국내에서는 아직 활성화되지 못하고 있다. 현재의 이동통신 시스템들은 주로 음성통신용으로 설계되어 있어서 데이타를 효율적으로 전송하는데 이들을 이용하는 것은 매우 어려우며, 동시에 많은 자원이 낭비되고 서비스의 품질 또한 저하되므로 무선 데이타통신 서비스에 대한 요구는 필수적이라 할 수 있다[5,6].

따라서 본 고에서는 ETSI RES 6 SC(European Telecommunications Standards Institute, Radio Equipment and Systems, Sub-technical Committee)에서 정의하고 있는 패킷모드 무선 데이타통신 표준인 TETRA(Trans-European Trunked Radio)와 패킷교환 무선 데이타통신을 위해 출현한 Ericssion사의 Mobitex 시스템을 바탕으로, 유선 통신망에 비해 그 안전성이 결여되는 무선 데이타 통신망의 무선 채널상에서의 정보보호 요구사항 분석과 대응책을 살펴보고자 한다.

2. 무선 데이타 통신

이제까지의 무선 이동데이타 서비스는 사설의 기술(Proprietary technologies)을 사용해 제공되어져 왔다. 휴대용 컴퓨터 장비의 폭발적인 증가, 각종 직무에로의 컴퓨터의 일반적 흡수, 그리고 어떤 조직체의 효율성 개선을 위한 무선 이동 데이타 통신의 중요성 인식 등은, 더 나은 성능과 효율적인 가격으로 서비스를 제공할 수 있도록 상호 작용하는 무선 이동 데이타 네트워크 구축에 큰 관심을 갖게 되었다. 유럽의 GSM(Group Special Mobile)과 같은 디지틀 셀룰라 전화는 현재 이동체 통신 개발의 가장 광범위한 분야를 차지하고 있으나, 이런 시스템들은 음성전화를 제공하고 회선교환 서비스로 데이타를 다

* 아주대학교 대학원 컴퓨터공학과 박사과정
** 아주대학교 대학원 컴퓨터공학과 석사과정
*** 아주대학교 컴퓨터공학과 교수

루도록 설계되어 긴 대화(session) 시간에 대해 간헐적인 짧은 메세지를 교환하고자 하는 경우 응용(applications)의 상당한 수정없이는 사용자에게 매우 값 비싼 서비스를 제공하게 된다. 예를 들면, 어떤 긴급 서비스를 제공하는 폐쇄적 사용자(closed user) 그룹내의 통신은 짧은 대화 설정 시간을 요하게 되므로 셀룰러 전화가 부적합하게 되는 특성을 갖게 된다[9,10]. ETSI는 이동 전화와는 다른 이러한 형태의 시스템이 필요함을 인식하고 trunked radio와 이동 데이타 시스템을 위한 공용표준을 개발하도록 활동하고 있으나, 무선 채널상에서의 안전성 위협요소는 하나의 걸림돌로 존재하게 된다.

가. 무선 이동 데이타 통신 구조

TETRA 무선 데이타통신 네트워크의 논리적 형태는 그림 1과 같으며, 인터페이스는 다음과 같다[9].

▶ Um(AIR-INTERFACE) : 사용자에게 서비스를 제공하기 위해 BS(Base Station)와 MS(Mobile Station)가 서로 작용하도록 하는 프로토콜.

▶ FNAP(Fixed Network Access Point) : 고정 사용자(Fixed user)와 고정망간의 인터페이스로 표준화된 인터페이스와 프로토콜을 사용하며, 장래의 이동 데이타 망은 이들 표준과 조화되어야 한다.

▶ MNAP(Mobile Network Access Point) : MTU(Mobile Terminating Unit)와 터미널 장치간의 물리적 인터페이스이며, 안테나를 장착한 노트북 컴퓨터와 같이 하나의 터미널 장비에 조합될 수 있다.

오늘날 대부분의 컴퓨터 통신은 peer-to-peer 통신이다. 즉, 호스트나 터미널의 응용 엔터티(application entities)간의 통신이다. 이것은 MNAP가 FNAP와 논리적으로 동일하다는 것을 의미한다. 다시 말해, MTU는 가입자에 의해 소유됨에도 불구하고 네트워크의 논리적 부분이 되는 것이다.

앞에서 언급한 세개의 인터페이스는 패킷 모드이며 air-interface는 유용한 데이타 트래픽을 위해 경제적 주파수 대역의 효율성을 가질 수 있다. 그러나, 이러한 air-interface는 무선 데이타통신에 있어서 한 BS 영역내의 모든 MS에 무선 채널을 공유하게 함으로 많은 위협 요소를 유발시키게 된다.

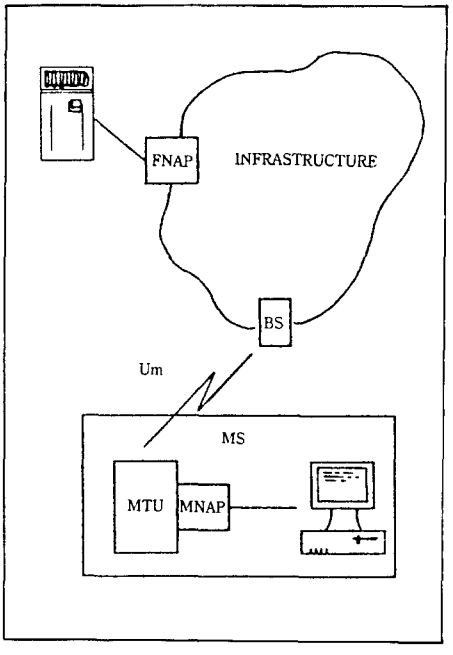
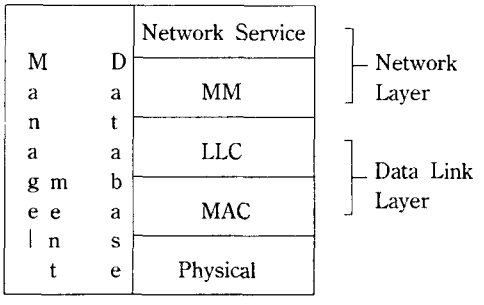


그림 1. TETRA network interface

나. 패킷 무선 데이타 프로토콜 구조

TETRA 무선 데이타 프로토콜을 위해 시험적으로 채택된 계층화 구조는 그림 2와 같으며, 그 윤곽은 LAN(Local Area Network)에 적합한 OSI 규약을 따르고 있다[9].



MM : Mobility Management
LLC : Logical Link Control
MAC : Medium Access Control

그림 2. 계층화된 프로토콜 구조

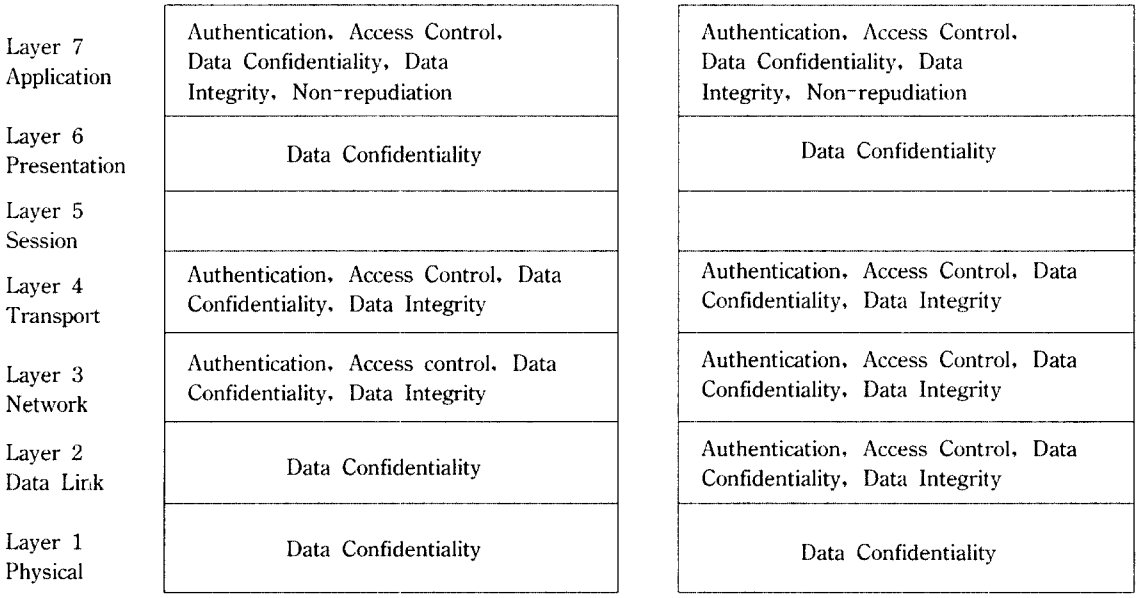
물리계층은 변복조 기능과 송·수신기 제어에 관련된 여러 기능을 통합한다. 데이타 링크 계층은 두개의 부계층으로 나뉘어지며, 방송 물리 채널(broadcast physical channel)의 멀티플렉싱과 디멀티플렉싱에 책임을 갖는 MAC 계층은 동기화(synchronization)를 담당한다. LLC 계층은 무선 링크를 통해 링크 계층 SDUs(Service Data Unit)의 정확한 전송에 책임을 지며, 패킷의 단편화, 조립, 전송 및 재전송과 같은 기능을 갖는다. 또한, 데이타 링크 계층은 무선채널의 안전한 전송을 위해 암호화 서비스를 수행할 수 있다. 네트워크 계층도 두 계층으로 나뉘어질 수 있으며 이동성관리 부계층은 이동체가 한 셀에서 다른 셀로 이동하였을 때, 그 하부구조(infrastructure)에 접속되는 가상 연결점을 유지하여 네트워크 서비스 부계층으로 부터의 PDU(Protocol Data Unit)를 흐름 제어할 수 있다. 네트워크 서비스 계층은 양단간(end-to-end) 네트워크 서비스를 제공한다. 마지막으로 관리 데이타 베이스는 수신된 신호강도, 에러율, 채널넘버, BS identity 등과 같은 항목의 파라메터를 포함한다.

3. 무선 데이타 통신망에서의 안전성 요구사항

앞절에서 살펴본 무선 데이타 통신망은 한 주파수 대역을 여러 가입자가 공유한다는 특성에 따라 LAN과 비슷한 면을 보이게 되고, 무선 채널상에서의 안전성에 있어 취약점을 가지게 된다. 우선 ISO 7498-2(Security Architecture)에서 제안하고 있는 안전성 서비스들의 계층적 배치를 살펴보면 그림 3.1의 (a)와 같으며[12], 무선 데이타 통신에 있어서는 (b)와 같이 적용할 수 있을 것이다. 이러한 무선 데이타 통신의 데이타 링크 계층에서의 안전성 서비스의 요구 사항을 특성별로 살펴보면 다음과 같다.

가. 데이타 전송 특성

무선 데이타 통신의 데이타 링크 계층에서 전송



(a) ISO 7498-2 Services (b) 무선통신에서의 서비스

그림 3.1 SECURITY SERVICES PLACEMENT

되는 PDUs는 WAN(Wide Area Network)에서와 같이 한번에 하나의 단일 링크를 통해 point-to-point로 전송되는 것이 아니라, 주어진 주파수 대역의 무선 채널을 통해 방송(broadcast)된다. 이러한 무선 채널을 통한 전송은 어느 BS의 영역내에 있는 모든 MS에게 가능하므로 다른 MS를 사칭하여 불법적 자원사용을 하거나 위장공격(Unauthorized resource use or Masquerade)을 할 수 있는 위협적 요소가 존재하게 된다. 그림 3.2는 이러한 특성을 보여준다.

따라서, 데이타 전송시 이러한 위협을 제거하기 위해 전송되는 메세지가 적법한 통신 상대로 부터 발신되었다는 증거를 필요로 하고, 통신하고자 하는 어떤 MS가 자원을 액세스하는데 있어 그 적법성 여부에 따라 제재를 가할 수 있어야 한다[1,2,7].

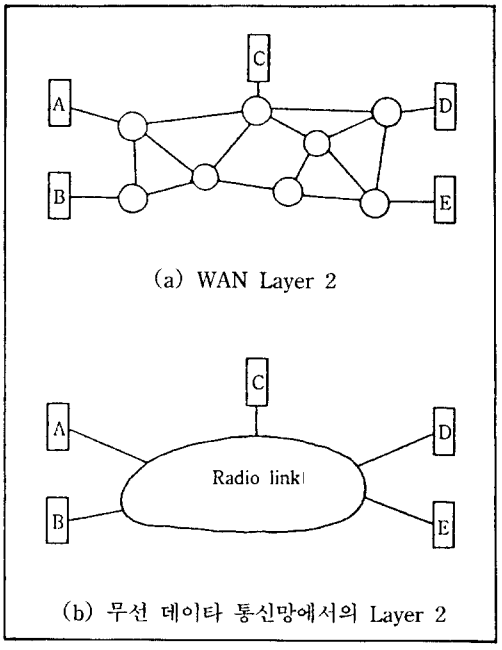


그림 3.2 데이타 링크 계층의 특성

나. 데이타 수신 특성

무선 데이타 통신에서의 데이타 수신시 하나의 BS영역에 있는 모든 MS들은 가. 절에서와 같은 무선 채널 특성으로 인해 데이타를 수신할 수 있다. 이러한 특성은 허가되지 않은 MS에게 정보가 누설(unauthorized disclosure) 될 수 있는 위협적 요소와 데이타 수정후(data modification) 재 전송될 수 있는 위협적 요소를 갖게 된다. 수신시, 이러한 위협을 제거하기 위해 부당한 MS가 도청을 하여도 그 내용을 파악할 수 없는 무의미한 상태가 되게하며 데이타를 발신시의 내용과 수신시의 내용이 일치하는지 검사함으로써 그 내용의 정확성을 기할 수 있다[13,14,15].

다. 주소 공간의 특성

무선 데이타 통신은 무선 링크의 방송(broadcast) 특성 때문에 무선 데이타 통신망의 주소가 계층 2의 무선 링크 채널상에서 유일해야만 한다. 이것은 주소가 정당한지 아닌지 일상적 관찰만으로 결정할 수 없다. 이러한 특성은 불법적인 MS가 자원을 사용하고(unauthorized resource use) 위장공격(masquerade)을 할 수 있도록 하는 위협 요소를 유발시키게 된다. 이 경우에도 역시 가. 절에서와 같이 전송되는 메세지와 전송하는 MS에 대한 적법성을 판단할 수 있어야 한다[15].

라. 무선 채널상에서의 위협요소와 서비스

앞에서 살펴보았던 무선 채널상에서의 여러 위협요소와 대응하는 안전성 서비스는 그림 3.3과 같이 나타낼 수 있다.

데이타 발신처 신분확인(Data Origin Authentication) 서비스는 불법적인 공격자가 적법한 다른 근원지 주소를 사용하여(masquerade) 데이타를 전송하지 못하도록 수신된 메세지에 그것이 정당한 발신처(source)로부터 발신 되었다는 확증을 갖도록 하는 서비스이며, 이는 위장공격(masquerade)의 위험을 줄이게 한다. 무연결 데이타 무결성(Connectionless Data Integrity) 서비스는 전송시 메세지의 변조을 방지하기 위해 단일의 무연결 PDU에서의 데이타가 부적절한 방법으로 변경되거나 파기되지 않도록 하는 특성을 제공하므로 데이타 변조의 위협을 줄이게 한다.

Threats	Services
Masquerade	Data Origin Authentication service
Data Modification	Connectionless Data Integrity service
Unauthorized Resource Use	Access Control service
Unauthorized Disclosure	Data Confidentiality Service

그림 3.3 위협요소와 서비스

액세스 제어(Access Control) 서비스는 불법적인 방법으로 자원의 사용을 할 수 없도록 자원의 인가되지 않은 사용에 대해 제재를 가하며, 데이타 비밀성(Data Confidentiality) 서비스는 인가되지 않은 개개인, 엔터티, 또는 프로세스의 도청에 대해 정보를 알 수 없게 하거나 누설되지 않도록 하는 특성을 제공하며, 이로 인해 불법적 정보의 누출 위험을 줄일 수 있다.

이러한 서비스들에 대한 메카니즘은 단일의 암호화 메카니즘을 통해 제공될 수 있다.

데이타 발신처 신분확인은 PDU 해더를 보호하는 암호화 체크섬 내에 발신처 주소의 암호화를 통해 제공될 수 있으며, 무연결 데이타 무결성은 데이타 필드를 보호하는 암호화 체크섬을 통해 제공될 수 있다.

또한, 액세스 제어는 암호화 제휴(Cryptographic associations. e.g., pairwise keys)의 관리를 통해 얻어질 수 있으며, 데이타 비밀성은 데이타 필드의 암호화를 통해 제공될 수 있다.

마. 무선 채널 보호를 위한 안전성 서비스 구조

이제까지 살펴보았던 무선 데이타 통신망의 무선 채널상에서의 안전성 서비스를 제공하기 위한 개괄적인 프로토콜 구조는 그림 3.4와 같이 나타낼 수 있다.

LLC와 MAC 계층 사이에 SRL 프로토콜 계층을 위치시킴으로서 무선 채널상에서의 안전한 데이타 교환을 수행할 수 있다. 이 프로토콜은 앞에서 언급

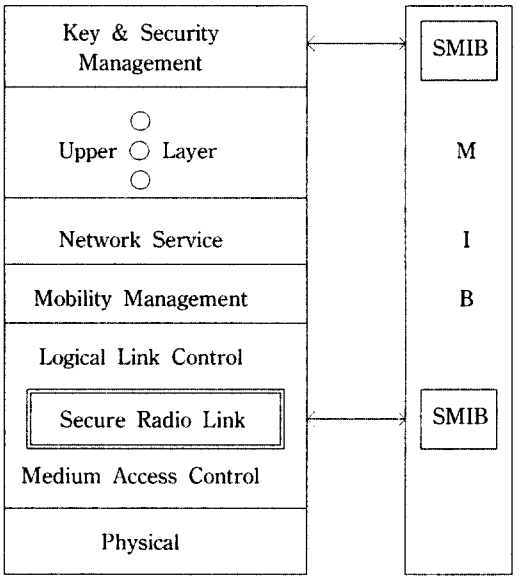


그림 3.4 안전성 프로토콜 구조

되었던 안전성 서비스들이 제공될 수 있도록 하며, SMIB(Security Management Information Base)를 통하여 키 관리 및 안전성 관리 응용과 통신할 수 있다. 이러한 프로토콜의 계층배치는 SILS(Standard for Interoperable LAN Security)에서와 같은 잇점에 따른다고 할 수 있다. 이것은 또한 상·하위 프로토콜 계층에 영향을 주지 않아야 하며, 안전성 서비스를 제공하지 않는 MS나 OSI에 따르는 고정망의 터미널과도 통신할 수 있어야 한다. OSI 계층으로 구성된 고정망과의 연동에 있어서는 키 분배와 같은 문제점들이 발생하게 된다. 그림 3.4에서의 프로토콜 구조는 무선 데이타 통신에 있어 무선 채널상의 안전성을 제공하기 위한 개괄적 구조에 불과하며, 키관리 및 안전성 관리, SMIB 구축, SRL의 프로토콜, 그리고 고정망과의 연동등은 세부적인 연구와 검토를 통해 이루어질 수 있을 것이다.

4. 결 론

아직 국내에서 활성화 되고 있지 못하는 무선 데이타 통신은 개인용 컴퓨터의 소형화 추세와 장소의

제약을 극복할 수 있다는 장점으로 인해, 그에 대한 요구는 점진적으로 증가되고 있다. 사용자에게 이동성을 부여한다는 측면에서 셀룰러 음성전화와 같은 일반화된 장비로는 데이타 전송에 많은 비효율적 요소가 존재함을 감안할때 무선 데이타 통신에 대한 요구는 필수적이라 할 수 있다. 그러나 유선통신에 비해 그 특성상 안전성이 결여되는 무선통신은 이러한 제약조건을 해결할 수 있어야 한다.

본 고에서는 무선 데이타 통신망을 위해 무선 채널상의 안전성 위협요소를 분석하고, 이에 대한 안전성 서비스를 제공하기 위해 OSI 7498 part 2 Security Architecture와 SILS(Standard for Interoperable LAN Security)를 기초로 해서 이에 대한 안전성 서비스 대책을 살펴보았다. 또한, 무선 채널상에 이러한 안전성 서비스들을 적용할 수 있는 개괄적 프로토콜 계층 구조를 구상해 보았으며, 이는 세부적인 연구와 검토를 통해 좀 더 연구되어야 할 것이다.

이러한 연구는 향후 무선 데이타 통신망의 가입자들에게 안전성을 보장해 줄 수 있는 토대로 제공하여 양질의 서비스와 함께 수요 창출의 걸림돌을 제거하도록 하며, 통신 시장 개방에 따른 대외 경쟁력을 다지는데 의의가 있다고 할 수 있다.

참 고 문 헌

1. Bransted, K.Dennis, "*Consideration for Security in the OSI Architecture*", IEEE Network Magazine, 1987.

2. C.H.Meyer, S.M.Matyas, "*Cryptography : A New Dimension in Computer Data Security*", John Wiley & Sons, 1983.

3. Communications & Marketing System, "*Wireless Access & PCN*", Vol.1~4, 1991. 1.

4. David J.Goodman, "*Cellular Packet Communications*", IEEE Transaction on communications, 1989. 8.

5. David J.Goodman, "*Trend in Cellular and Cordless Communications*", IEEE communications Magazine, 1991. 1.

6. Donald C.Cox, "*Portable Digital radio Communications-an Approach to Tetherless Access*", IEEE Communications Magazine, 1989. 7.

7. D.E.Denning, "*Cryptography and Data Security*", Addison Wesley, 1982.

8. John loannidis, Dan Duchamp, "*IP-based Protocols for Mobile Internetworking*", ACM. 1991.

9. John L Haine, Paul M Martin, Rupert L A goodings, "*A European Standard for Packet-Mode Mobile Data*", PIMRC'92, pp.513-519.

10. K.Parsa, "*The Mobitex Packet-Switched Radio Data system*", PIMRC'92 pp.534-538.

11. W.Diffie, M.Hellman, "*New Direction in Cryptography*", IEEE Trans. Information Theory, Vol.IT-22, No.6, Nov., 1976.

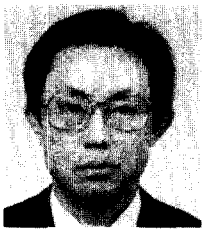
12. "*ISO* 7498/2 *Part* 2 *to ISO* 7498 *on Security Architecture*", ISO/TC97/SC21/WG1, 1987.

13. "*Standard for Interoperable LAN Security*", IEEE 802.10, Dec., 1989.

14. 김동규 외, "OSI 통신망 구조에서의 네트워크 안전체제 연구", 과학기술처 최종 보고서 (3차 년도), 아주대, 1991. 6.

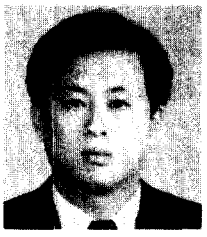
15. 김동규, 임병렬 외, "디지탈 셀룰라 네트워크에서의 안전성에 관한 연구", 한국통신 정보보호학회 학술발표회, 1992. 11.

□ 著者紹介



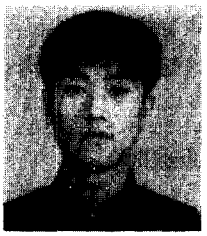
金 東 圭

1947年生
서울 大學校 工科大學 卒業(學士)
서울 大學校 自然科學大學院 卒業(碩士)
美國 KANSAS 州立大 大學院 卒業(Ph.D. 電算學, 情報通信 專攻)
美國 KANSAS 州立大 電算學科 教授
現　在 : 亞洲大學校 컴퓨터工學科 教授
著　書 : 데이타 통신 시스템, 회중당, 1986년
컴퓨터 통신 네트워크, 상조사, 1988년
關心分野 : 컴퓨터 네트워크, 정보통신 프로토콜 엔지니어링,
정보통신 Security, 분산처리 시스템



林 炳 烈

1963年生
1991년 2월　全北產業大學校 電算學科 卒業
1993년 2월　亞洲大學校 大學院 電算學科 卒業
1993년 3월～현재　亞洲大學校 大學院 컴퓨터工學科 博士過程



羅 種 根

1970年生
1992년 2월　亞洲大學校 電算學科 卒業
1992년 2월～현재　亞洲大學校 大學院 컴퓨터工學科 碩士過程