2002 한국정보통신설비학회 하계학술대회 논문집 2002. 8. 30-31

무선 통신을 사용한 모니터링 시스템의 설계 및 구현

전윤호, 우종현, 김영륜, 김희동
한국 외국어 대학교 정보통신공학과

Monitoring system design&Implementation using wireless solution

Yoonho Jeon, JongHyun Woo, YoungRyun Kim, HeeDong Kim
Dept. Information and Communication Eng. Hankuk University of Foreign Studies

Abstract - RS-232C는 정보기기들을 연결하는 직렬통신 표준으로, 간단한 구조로 인해, 복잡한 요구 조건이 없는 상용 기기들의 제어 및 감시용으로 사용되고 있다. 최근 무선통신기술이 발전함에 따라, 저가격의 무선통신 기술을 활용하여 무선 RS-232C에 대한 요구가 늘어나고 있다. 무선 RS-232C로 기존 유선의 RS-232C를 대체함으로서, 기존 시스템의 변경없이 편리한 접속기능을 대체할 수 있을 것이다. 본 논문에서는 유선 RS-232C를 대체하는 무선 RS-232C 모듈을 채용하여, 전력제어에 사용하는 배전자동화 장치의 관리를 간편하게 하는 시스템의 구현에 대해서 다루고 있다. 배전 자동화시스템은 일종의 SCADA시스템의 일부로서, 통신 프로토콜로서 산업용 DNP3.0을 사용하고 있다. 무선 RS-232C 링크의 신뢰성을 확보하기 위하여, 무선 구간에 DNP3.0을 채택하였으며, 무선 통신방식으로는 무선 RF, 블루투스(Bluetooth), 무선랜(wireless LAN)등 3가지 방식을 채용하여, 설계, 구현내용을 기술하였다.

1. 서 론

최근의 산업용 기기들은 마이크로 프로세서를 내장하고, 다양한 기능을 수행하고 있으며, 이 기기를 관리 및 유지 보수 또는 원격 제어를 위하여 유선 통신에 의한 RS-232C 비동기 통신하는 경우가 대부분이다. RS-232C의 I/O를 자사의 제품에 채택한 많은 업체들은 무선 솔루션으로 대체함으로써 자사 제품의 기능향상과 차별화를 꾀하고 있다. 상황에 따라서는, 유선은 무선으로 대체함으로써 위험한 산업 현장에서 근무자를 보호할 수 있고, 또한 빠른 접근성 및 시스템 설립 능력을 확보할 수 있으며, 운영 유지 보수의 편리성을 도모할 수 있다.

본 논문에서 근거리 무선통신 방식에 의한 무선 RS-232C 구현하고자 한다. 무선 RF모듈, 블루투스(BlueTooth), 무선랜(wireless LAN) 세가지 방식에 대하여서 구현하였으며, 각 방식에 대한 설계 구현 내용을 기술하였다. 본 논문의 대상이 되는 시스템은 배전 자동화에 사용되는 시스템인 FRTU-P100(Feeder Remote Terminal Unit)로서, 전신주위에 설치되어 운용됨으로써, 운영유지보수를 위해서는 RS-232C포트를 연결하기 위해서, 관리자가 전신주 위를 올라가야 하는 번거로움을 없애고, 무선으로 원격제어기능을 수행할 수 있도록 함이 목적이다. 유선 RS-232C를 무선RS-232C로 변경하기 위해서는, 기존 시스템을 그대로 두고 유선 포트사이를 무선으로 대체하는 방법과, 시스템의 내부를 수정하여 무선 interface를 내장하는 방법을 모두 고려하였다.

한편, 무선 RS-232C의 무선구간에서의 신뢰성이 있는 통신을 위해서, 무선 링크의 채널오류를 극복하도록 하는 링크계층으로서 DNP3.0 프로토콜을 채용하였으며, 보안성을 위해서 인증기능을 추가하도록 하였다. 여기서, DNP3,0 프로토콜은 전력계통의 SCADA에 사용되는 통신프로토콜로서, 시스템 내부에 이를 채용하고 있으므로, 기존 프로토콜을 무선 링크에 삽입함으로써, 추가 관리 기능을 사용할 수 있는 장점이 있다.

서론에 이어, 2장에서는 무선 RS-232C의 설계의 고려사항을 기술하고, DNP 프로토콜의 링크계층을 간단히 설명한 후, 3,4,5 장에서는 무선RF모듈, 블루투스, 무선랜 기술을 이용한 시스템의 설계에 대해서 기술하였다. 마지막으로 6장에서 결론을 맺는다.

2. 무선 RS-232C의 개요

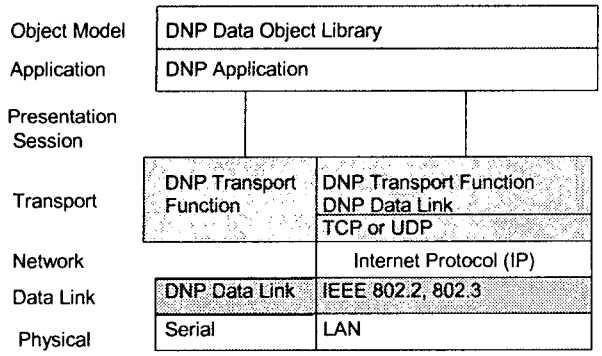
유선과는 달리 공중 매체는 사용상 국내 전파법의 제한을 받으므로, 국내 전파법을 만족시키는 대역안에서 구현하여야 한다. 비허가 주파수 대역으로는 424.7~424.95MHz대역과 2.4GHz 대역의 ISM밴드를 사용할 수 있다. 424MHz대역은 주파수 대역이 좁아 낮은 전송속도이나, 블루투스나 무선 LAN이 사용하는 2.4GHz대역은 고속의 전송이 가능하다.

본 논문에서 실제적인 사례로 사용되는 RTU에서의 요구 조건은 최소 2400bps의 속도, 연동거리 10 ~ 50m 구간에서 사용이 가능해야 한다. 또한 향후 상용 제품으로의 전환 가능성을 고려하여, 비용적인 측면을 고려하면서 구성해야한다.

한편, 블루투스나 무선LAN을 사용하는 경우에는 프로토콜 스택이 있어, 채널오류를 극복하도록 구성할 수 있으나, 무선RF모뎀을 사용하는 경우에는 채널오류를 보정하고, 링크의 효율적으로 사용하기 위한 링크계층이 필요하게 된다. 본 논문에서는 DNP3.0의 프로토콜 스택을 구현함으로써, 채널오류 특성을 개선하도록 구성하였다. DNP3.0의 프로토콜 스택을 OSI 7계층 참조모델과 비교하여 <그림 1>에 나타내었다.

<그림 1>의 왼편 부분인 DNP 기본구조는 물리, 데이터링크, 응용계층의 3계층을 기본으로 하며, 이를 EPA(enhanced performance architecture)라 부른다. 이와 같이 계층을 줄인 것은 계층간의 인터페이스를 위한 오버헤드를 줄이고 효율적인 통신기능을 수행하기 위함이다. EPA에서는 응용계층에서의 메시지단위가 255옥텟 이내로 모든 프레임이 정의되어 있었으나, DNP는 여기에. 파일전송 응용 등과 같이 긴 프레임을 전송할 수 있

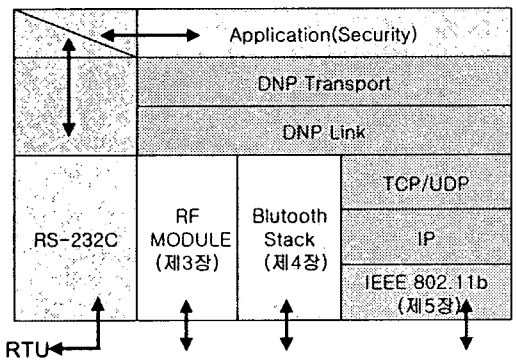
도록 프레임의 분할과 조합기능을 하는 트랜스포트 기능을 추가함으로써 DNP의 응용영역을 확장할 수 있도록 배려하였다.



<그림 1> DNP 3.0 의 프로토콜 스택

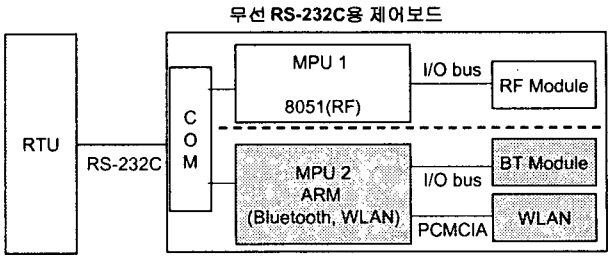
한편, <그림 1>의 오른편 부분은 LAN 및 인터넷을 통하여 제어할 수 있도록, 물리계층부분을 IEEE802.3, IP, TCP/UDP를 대체된 형식으로, TCP 상위에 DNP 데이터링크가 올라가도록 되어 있다. 본 과제에서는 표준에 따라 하위계층에 WLAN을 사용할 수 있다.

<그림 2>에는 본 연구에서 제시하는 3가지의 무선 RS-232C에 대한 프로토콜 스택을 나타내었다. RF 모듈의 무선구간의 신뢰성을 확보하기 위해서, RTU에서 사용하는 DNP 프로토콜 스택을 사용하는데, 특히, DNP3.0의 데이터 링크는 최대 255옥텟을 프레임 단위로 하는데, 헤더 필드 10옥텟에 2옥텟의 CRC를 부가하고, 데이터에도 16옥텟마다 2옥텟의 CRC를 부가하여 해밍거리를 6으로 확장하여 신뢰성있는 데이터링크를 확보하도록 설계되어 있다. 이와 같이 DNP가 실장됨으로써, RS-232C포트를 이용하여 SCADA 통신용으로 사용할 수 있게 됨으로써, RTU입장에서는 백업라인을 확보하는 부수적인 효과도 얻게 된다. 또한, 블루투스 및 WLAN에도 상위계층에 DNP를 사용하으로써, 공통성을 높이고 있다.



<그림 2>. 무선 RS-232C system Stack 구조

본 연구에서 구성한 하드웨어는 3가지 종류로서, <그림 3>에는 이들의 블록도의 함께 나타내었다. 우선 RF모듈의 경우, 제어가 간단하므로 소형 싱글칩 프로세서인 8051을 사용하고, I/O 버스를 이용하여 모듈과 인터페이스 한다. 블루투스나 WLAN의 경우는 프로토콜 스택이 비교적 복잡하여, ARM 프로세서를 채택하되, 블루투스 모듈과는 I/O 버스로, WLAN모듈과는 PCMCIA로 접속한다. 이어서, 각 모듈에 대해서 설명하도록 한다.



<그림 3> 무선 RS-232C System의 H/W Block Diagram

3. 무선 RF 모뎀

무선 RS-232C의 구현에 필요한 RF 모듈은 국내 전파법에 규정한 기술기준에 적합한 저가형 상용모듈을 사용하도록 한다. Hardware적으로는 MPU의 I/O port와 hand shaking 방식의 규정을 맞추고, 이를 제어하기 위해 software적으로 RF module의 주파수 설정 및 동작 mode 설정을 위한 status register 값을 setting하면 된다. 사용주파수 대는 424.700 ~ 424.950MHz 대역으로, 채널대역폭은 8.5KHz이하이며, 대역폭이 좁은 만큼 전송속도는 1200/2400bps 로서 비교적 낮다. 동작 모드로는 Half duplex를 사용하도록 한다.

MPU는 앞서 설명한 바와 같이 DNP 3.0 프로토콜을 구현하는데, RTU입력되는 RS-232C 비동기 데이터를 수신하여, CR(carrage return), LF(line feed)까지를 하나의 블록으로 묶어서, DNP의 응용계층으로 넘기면, 응용계층에서는 바로 트랜스포트계층으로 바이패스한다. 트랜스포트에서는 255블럭길이로 나누어 프레임을 분할하고, 이를 데이터링크계층으로 내리면, 프레임을 형성하여 모뎀으로 전송하되, 이 과정에서 링크의 형성 및 제어를 위해서 제어프레임을 사용한다. 수신은 이의 역순으로 진행된다. 다만, DNP에서는 대칭모드를 지원하고 있으므로, 모니터 단말측에서 Unsolicited message frame이 송신되어 충돌이 발생할 수 있으나, 이는 프레임상에서 해결하도록 한다.

4. Bluetooth

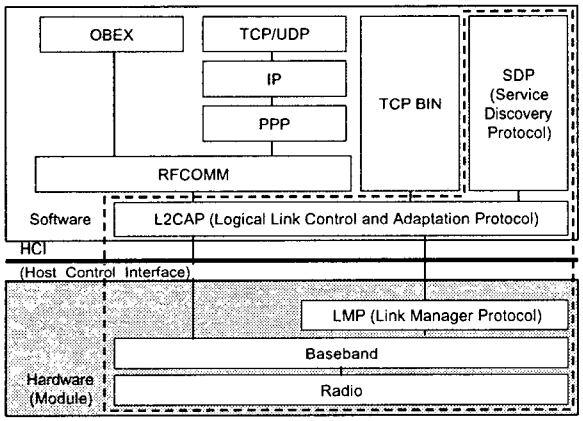
4.1 Bluetooth 기본 개념

Bluetooth는 2.4GHz ISM band를 사용하여 이동 전화와 이동식 장치 등의 근거리 통신을 위해 최적화된 기술방식이다. Bluetooth는 기기 간에 master와 slave의 관계를 가질 수 있으며, master는 piconet 또는 PAN (Personal Area Network)라 불리 우는 영역의 slave를 7개까지 제어하게 된다. 또한, 기기 간의 다른 AP (Access Point)를 거쳐 통신할 수 있으며, AP를 거치지 않고 직접적인 통신이 가능한 Ad-Hoc 방식도 지원하고 있다. 거리는 일반적으로 10cm~10m이나 100m까지 확장이 가능하다. 최대 1600hops/s의 FHSS을 사용하여 기기간의 간섭영향을 최소화하고 있으며, TDD를 사용하여 링크를 구성하고 있다. piconet의 활동하지 않는 기기는

저전력 모드(sniff, park, hold)로 변하게 된다. 기기 간의 보안을 위해 128bit의 인증(authentication) 키와 암호화(encryption) 키를 사용하고 있다.

4.2 bluetooth Stack

Bluetooth Protocol Stack은 <그림 4>에 나타낸 바와 같이, 상용 Chip으로 구현된 Hardware Stack과 Software로 구현되는 Stack으로 나뉘어 지며, 이들 사이에는 HCI(Host Control Interface)가 정의되어 있다. 점선 부분은 Bluetooth 고유의 기능을 하는 Core protocol (Baseband, LMP, L2CAP, SDP)를 나타낸 것이다. 한편, 블루투스에서는 범용의 프로토콜을 사용하도록 할 때, 버전의 차이로 인한 상호호환성이 결여될 수 있는 우려가 있어 모든 프로토콜 스택을 번들로 처리하고자 풀스택을 사양으로 정의하고 있다. 많은 응용이 예상되는 직렬 송수신을 위한 RFCOMM을 두고 있으며, 이 위에 무선 전화 기능을 제공하는 TCP BIN(Telephony Control Protocol Specification - Binary), 그리고 Application을 제공하는 OBEX(Object Exchange), PPP, IP, TCP/UDP 등이 존재한다. <표 1>은 각각의 Block에 대한 기능을 간단히 설명하고 있다.



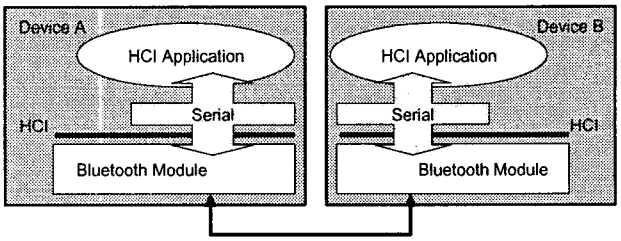
<그림 4> Bluetooth Stack

<표 1.> Bluetooth Protocol Stack의 요소들

Protcol	설명
Baseband	Bluetooth 탑재기기 간의 접속 시 호핑 주파수와 클럭의 동기화
LMP	암호화 키 생성 및 교환, 접속 상태 제어
HCI	Software와 Hardware 사이의 데이터 Flow control 및 Message 정의
L2CAP	데이터의 분할 및 조합, 상위 Protocol로의 데이터 송수신 기능
SDP	Bluetooth 이용용도를 미리 결정
RFCOMM	RS-232C 등의 시리얼 송신 컨트롤
TCP BIN	호출 제어신호 규정 및 Bluetooth 기기 간의 그룹 관리
PPP	Point -to-point 접속 확립
IP/TCP/UDP	IETF에 정의된 Internet Protocol
OBEX	Object 교환을 위해 IrDA에 의해 정의된 session Layer 역할

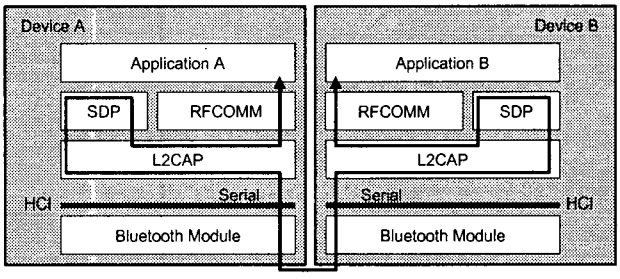
4.2 Bluetooth 구현 방향

무선 RS-232C를 Bluetooth 기술을 채용함에 있어 하드웨어 구성은 < 그림 3>과 같이 RF 모듈을 Bluetooth로 대체하는 정도이다. 소프트웨어의 측면에서의 방법은 대개 3가지 방안이 있을 수 있다. 첫째, 앞서 RF module을 이용하는 것과 같이 Bluetooth의 RF기능의 Module 만을 이용하는 방법과, Bluetooth Hardware Chip을 HCI Interface를 통하여 소프트웨어로 제어하는 방법(그림 5 참조), 마지막으로 RFCOMM위에 직렬 통신 응용을 올리는 방법(그림 6. 참조) 등이 있다.
첫 번째 방법은 초기에는 블루투스 RF모듈이 분리되어 시판되었으나, 최근에는 원칩으로 개발되어 Bluetooth RF module만을 구입하기 어렵고, 비교적 계층간의 Interface가 복잡하여 구현의 경제성이 없다.
두 번째 방식은 상위계층은 구현하지 않고, 블루투스의 RF와 링크관리 프로토콜 인터페이스까지를 HCI를 통하여 제어하는 방법이다. Bluetooth의 기본적인 Inquiry (device를 조회, 정보 취득)와 Connection (device와의 접속) 만을 구현하여 Ad-Hoc 방식을 이용한 두 기기 간의 통신이 가능하다. 이런 경우, 다른 기기와의 호환성 문제가 있을 수 있으나, 본 개발에는 호환성이 필요한 부분은 아니므로, 문제는 없다.



<그림 5> HCI를 통한 블루투스 Module 컨트롤

세 번째 방식은 기존의 Serial Port Profile을 사용하여 구현하는 것이다. 수신의 경우, 데이터가 모듈을 통하여 들어와, L2CAP에 의해 데이터를 분할 및 조합하여 SDP에 의해 Serial 통신을 결정하게 되고 RFCOMM에 의해 상위 Application과 통신하게 되며, 송신의 경우 반대로 이루어진다. <그림 6>에서 Serial 통신의 모습을 보여주고 있다. Bluetooth Module은 CF 타입을 사용할 것이며, 리눅스용 Bluetooth Stack을 사용하고자 한다.



<그림 6> Serial Port Profile

5. 무선랜

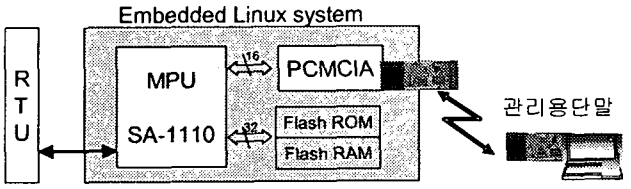
5.1 WLAN 기술의 장점

최근 급속히 보급되고 있는 IEEE 802.11b는 2.4 GHz 대역에서, 약 11Mbps 전송 속도를 제공한다. 공중통신 사업자들은 공중 무선LAN사업을 위해 Hot Spot지역에 Access Point(AP)를 설치하고 있으며, 향후 3세대 이동통신인 IMT-2000과 함께 초고속 무선접속 서비스의 주류를 이룰수 있는 기술로 예측되고 있다. 무선RS-232C의 어댑터로서 WLAN 기술을 채용하는 것은 현시점에서는 경제성이 없으나, WLAN의 가격은 하락되면 경제성도 얻을 수 있다. 또한, RTU는 경우에 따라 Hot Spot 지역에 설치될 경우도 있으므로, RTU에 WLAN 접속 Interface를 설치함으로써 RTU의 제어관리는 물론 SCADA의 통신 회선으로 활용할 수 있는 장점이 있다. RTU에 장착된 WLAN station은 제어용 모니터와는 Ad-hoc mode으로, SCADA 통신 회선과는 인프라스트락쳐 모드로 mode로 동작하게 된다.

5.2 무선랜을 사용한 설계

WLAN의 통신 기능을 부여하기 위해서는 <그림 3>에 나타낸바와 같이 RS-232C로 연결되는 별도의 접속 모듈을 개발하는 방법과 RTU 내부에 WLAN 접속 기능을 구현하는 방법이 있다. 후자의 방법은 궁극적인 구성 방법으로 RTU의 Hardware를 변경하여야 한다. 소프트웨어적으로도 RTU는 현재 실시간 운영체제인 μC/OS 기반으로 되어 있어, PCMCIA 및 802.11b Driver 구현이 필요하게 되는 단점이 있다. 반면, 전자의 경우는 별도의 하드웨어에 상용 운영체제를 사용할 수 있어, 드라이버를 별도로 작성할 필요가 없는 장점이 있다. 따라서, 본 논문에서는 전자의 방법으로 기본 기능을 구현하고, 추후 RTU의 하드웨어 및 OS를 변경할 계획이다.

출시된 무선랜 모듈은 PCMCIA 타입의 무선랜 카드를 활용하는 방법을 사용하였다. 이러한 PC-card 형태의 디바이스를 손쉽게 제어하기 위하여 내장형 리눅스(Embedded linux)를 선택하였다. 내장형 리눅스는 커널과 모듈을 합하여 600k가 넘지 않는 매우 작은 형태의 OS이지만, 각종 네트워크 디바이스의 드라이버 등을 지원하므로, network 응용을 개발하기 적합하다. <그림 7>에는 대략적인 하드웨어 구성도를 나타내었다.



<그림 7. 무선랜을 사용한 하드웨어 구성도>

MPU로는 최근 출시되어 PDA등에 많이 사용되는 Intel의 StrongARM Processor인 SA-1110을 채용하고, FlashROM을 사용하여 Embedded OS와 응용프로그램을 탑재시킨다. OS에는 PCMCIA 모듈과 802.11b 모듈이 내장되어 있다.

WLAN을 사용하는 경우의 프로토콜 스택은 <그림 2>에 나타낸 바와 같이, TCP/ UDP 위에 응용프로세서로서 DNP 3.0 프로토콜 스택을 올리는 형태이다. TCP와 UDP는 ad-hoc mode에서는 private IP로 통신을 하고, Infrastructure mode에서는 해당 AP로부터 DHCP 할당을 하여 동작한다.

6. 결 론

본 논문에서는 운영관리의 편리성을 위해서 기존의 유선 RS-232C를 무선 RS-232C로 대체하는 방법을 고려하였다. RF모듈, 블루투스, WLAN의 3가지 방법을 모두 고려하였으며, 이에 대한 하드웨어의 구성과 소프트웨어 프로토콜 스택을 제시하였다. 특히, 무선 RS-232C채널의 신뢰성을 확보하기 위해서, RTU에서 사용하고 있는 프로토콜인 DNP3.0을 채택하였으며, 이로 인해서 SCADA시스템의 백업채널을 확보할 수 있었다. 현재, 시스템을 구현중에 있으며, 구현 시간을 단축하기 위해서 구입가능한 현재의 솔루션등을 최대한 활용하는 방향으로 진행하고 있다.

RF모듈에 의한 방법은 전파법에서 규정한 기술기준을 만족시켜야 하며, 전송속도와 전송거리 면에서 최소의 성능을 나타내지만 경제적으로 구현할 수 있다. 한편, 블루투스와 무선랜은 전송속도에서 우수하고, 무선링크의 신뢰성도 확보할 수 있고, RTU의 확장성도 우수하지만, 현재로서는 비용이 소요되는 단점이 있다.

본 과제를 통하여 최근 각광받고 있는 무선 기술을 모두 시험해 보는 경험을 얻게 되었고, 곧 현장에 적용될 것으로 기대된다.

[참 고 문 헌]

[1] 임명섭, "Wireless LAN Modem 기술", KRNET2002, 2002년
[2] 이응혁, "8051 마이크로컨트롤러 프로그래밍과 인터페이싱", 사이텍미디어, 2002 1월.
[3] (주)팜팜테크, TynuxII User Guide, 2002.
[4] W.S. KANG, "Introduction of Bluetooth Technology" August 30, 2000
[5] Seecode BlueTooth pds (http://www.seecode.com/f_list.php3?code=f_board)
[6] Bluetooth home sitev.1.1.core (http://www.bluetooth.com/dev/specifications.asp)
[7] Geier , "Wireless LANs 2nd Edition", 2001.
[8] DNP 3.0 Protocol Specification.