PC 환경에서 시뮬레이션 기능을 포함한 블루투스 프로토콜 분석장비

(A Bluetooth Protocol Analyzer including Simulation Function based on PC Environment)

정 중 수 †

(Joong-Soo Chung)

요 약 오늘날 무선통신 기술은 기존 유선 통신방식과 더불어 매우 주목받고 있는 정보통신 혁명을 주도하였다. 무선 통신에서 자체 피코넷을 형성하여 음성이나 데이타 통신을 수행하는 블루투스 기술은 이제 액세스망을 통해 공중망과 접속 가능하게 되었다.

본 논문에서는 블루투스 디바이스와 UART 케이블로 접속된 PC 환경에서 블루투스 프로토콜을 분석하는 블루투스 프로토콜 분석장비 개발을 소개하였다. 이의 개발 환경으로는 윈도우 98 OS와 MS 비주얼 C를 사용하였다. 비주얼 C로 작성된 응용 프로그램은 블루투스 디바이스에 실장된 펌웨어와 인터페이스를 수행하여 개발되었다. 또한 개발된 시스템으로 실제 음성 시험을 위하여 시그널링 용으로 헤드셋을 사용하고, 파일 전달용으로 PC를 사용한 블루투스 시스템간 프로토콜 정보를 시뮬레이션 하였다. 시뮬레이션은 하드웨어인 디바이스와 소프트웨어가 실장된 PC 간의 UART 통신의 속도는 다양하게 변화가능하나 약 20kbps 이하의 속도를 제외하고는 성능에 영향을 거의 주지 않았으므로 한계치인 115kbps로 시험하였다. 성능해석은 블루투스 시스템간 파일 전달시 처리량을, 헤드셋과의 통신은 호 설정 시간과 해제시간을 성능분석 파라메터로 제시하였다. 이때 파일 전달은 개발된 소프트웨어에서 파일 액세스 하는 주기적인 시간이 매우 큰 의미가 있었다. 액세스하는 파일의 패킷 크기는 가변이나 통상 많이 사용하는 128 바이트로 고정하고 시험 한 결과, 주기적인 파일 액세스 시간이 0.04초일 때 약 13kbps 처리량을 유지하는 블레이크 포인트 시간이었다. 헤드셋과의 통신시 호 설정 시간과 해제시간은 약 16.6ms가 소요된다. 따라서 이와 같은 결과는 실제 블루투스 시스템이 저속의 파일전달이나 음성 정보전달을 위한 시그널링 용의 장비 개발 시 충분한 성능 검증용으로 활용될 수 있다.

키워드 : 블루투스, 프로토콜 분석

Abstract In addition to wired communication technology, wireless communication technology has had communication revolution nowadays. Bluetooth technology carries out data/voice communication within pico-net. Nowadays the various services are supported by access network connected to public network.

This paper presents implementation of bluetooth protocol analyzer which simulates bluetooth protocol. MS window98 and visual C are used for development environment and application program is operated over the firmware loaded on the bluetooth device connected to the PC through UART which of the maximum transmission rate is 115kbps because tranmission rate less than 20kbps affects rarely the performane. The performance analysis on the proposed system is carried out as simulating the signalling information for the voice test and the traffics between two bluetooth systems for file transfer. The throughput analysis for file transfer service and call processing capacity for voice service are considered as performance analysis parameters. File access time is very important parameter and throughput is 13 kbps in case breakpoint time to file access is 0.04sec. Also call processing time

· 본 연구는 한국연구재단 산학협력 지원 사업으로 수행되었습니다.

† 정 회 원 : 안동대학교 전자정보산업학부

jschung@andong.ac.kr

논문접수 : 2002년 8월 5일

심사완료 : 2002년 11월 9일

is about 16.6ms in case of communication with the headset. The performance analysis of simulation results satisfies with bluetooth device development.

Key words : Bluetooth, Protocol Analysis

1. 서 론

종래 유선 통신망은 전화교환망(PSTN: Public Switched Telephone Network), 패킷교환망(PSPDN: Public Switched Packet Data Network), ATM(Asyn chrobous Transfer Mode) 등으로 진화되고 있으며, 무선 통신망은 이동통신망을 중심으로 진화되었다. 특히 블루투스 기술은 하드웨어와 펌웨어가 어떤 종류이고, 어떻게 구성되는지 몰라도 소프트웨어와 특정한 송, 수신패킷을 정의함으로써 하드웨어(펌웨어 포함)와 소프트웨어 독립성을 보장하여 쉽게 개발자들이 접근하도록 하였다. 케이블 없이 가전기기, PC 장비, 전화기 종류 등을 연결하는 블루투스 기술은 최근에 그 권고안[2]이 확정되어 전 세계적으로 붐을 타고 있는 실정이다. 이와 같은 무선통신 관련 블루투스 트래픽 분석장비는 블루투스 기술을 이용한 시스템 개발에는 필수적이나 현재 이러한 프로토콜 분석기는 활용성이 많음에도 불구하고 국내외 개발 제품은 거의 없는 실정이다. 특히 국내 제품은 전무하고, 수입하는 장비로서는 PC 본체에 윈도우 98 위에 소프트웨어를 탑재하는 경우[3]가 있으나 이들은 일반적으로 성능면에 비해 고가이다.

본 논문에서는 무선통신에 사용되는 블루투스 프로토콜 분석기 개발을 블루투스 프로토콜 스택 인증을 위한 문서[4]에 근거하여 전반적인 설계 기법의 제시와 개발 과정 및 성능 분석을 수행하였다. 블루투스 프로토콜 분석기의 개발 환경으로는 펜티움 II 프로세서 800 MHz PC 기반의 윈도우 98 OS와 CSR회사에서 제공되는 펌웨어 10.3 버전의 환경하에서 수행되는 MS 비주얼 C를 사용하였다.

설계과정을 살펴보면 먼저 프로토콜 분석기에 관련된 하드웨어 주변장비들을 구입하여 USRT로 PC에 접속하여, PC 호스트(편의상 PC로 명하였음)위에서 소프트웨어 구성요소들을 블록단위로 나누어 개발하였다. 또한 개발된 시스템의 점검을 위해 두 대의 블루투스 시스템끼리 통신을 수행시키면서 파일 전달시을, 헤드셋과는 음성전달을 위한 호처리를 수행하였다. 아울러 파일 전달시 처리량을, 헤드셋과의 통신시 호 설정 시간과 해제 시간을 성능 분석 파라메터로 제시하였으며, 그 결과 만족한 성능을 수행하였다.

2. 블루투스 프로토콜 분석기 환경

블루투스 시스템의 구성형태는 그림 1과 같이 크게 블루투스 하드웨어와 관련된 부분과 소프트웨어 프로토콜 스택으로 나눌 수 있다.

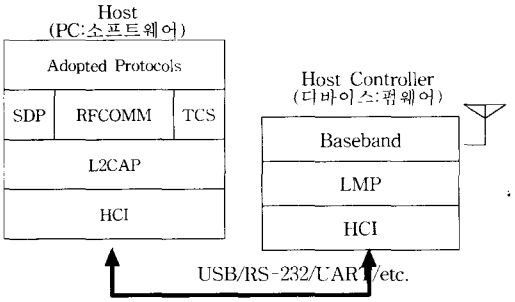

그림 1 블루투스 시스템의 프로토콜 스택

하드웨어와 관련된 부분은 블루투스 칩이나 모듈을 만드는 업체에서 펌웨어와 하드웨어 구성도가 이미 상당히 공개되었으며, 일반 블루투스 애플리케이션 개발자들에게는 그것들을 활용만 하면 된다. 이 펌웨어 부분은 블루투스 스펙 설명서[2]의 상당 부분을 차지하고 이해하기에 상당히 난해하다. 펌웨어가 대부분 플래시 타입의 메모리에 저장돼 있다가 호스트에서 내려오는 명령을 받아 내부적으로 처리할 수 있으면 처리하고 외부 RF로 보낼 필요가 있을 때는 LM에 의해 상대 디바이스에 명령를 송수신한 후 결과인 이벤트를 PC로 올려주게 된다. 이러한 펌웨어는 다음과 같이 구성된다.

- 베이스밴드 펌웨어: 블루트스 하드웨어의 핵심이랄 수 있는 베이스밴드 하드웨어를 직접 제어한다.
- LM(Link Manager): 블루투스 시스템이 통신시 링크 관리부이다.
- LMP(Link Manager Protocol): 링크 관리를 위한 프로토콜이다
- HCI(Host Controller Interface) 호스트 컨트롤러 파트: UART나 USB로 접속되어 PC에 로딩된 블루트스 애플리케이션 소프트웨어에서 수신되는 HCI 명령을 해석하여 LM과 연동해 적절한 명령을 수행한다.
- UART/USB 인터페이스 펌웨어: 호스트와 데이타

를 주고받는 인테페이스 하드웨어를 직접 제어하는 부분이다.

나머지 PC에 로딩될 소프트웨어 프로토콜 스택의 기능을 간략히 언급해 보면 다음과 같다.

• HCI 호스트 인터페이스: 블루투스 모듈(편의상 디바이스로 명하였음)과의 표준 인터페이스 방법을 정의하고 있다.

• L2CAP(Logical Link Control Adatation Protocol): 블루투스 환경에서 논리적인 커넥션을 만들어주고, 커넥션시 데이타를 전송하는 기능을 한다.

• SDP(Service Discovery Protocol): 블루투스 디바이스가 제공하는 서비스의 종류를 검색할 수 있는 방법에 관한 프로토콜이다.

• RFCOMM: 시리얼 포트를 시뮬레이션하기 위한 기능

• TCS(Telephony Control Service): 무선 전화 기능을 블루투스에서 구현하기 위한 프로토콜이다.

• Adopted Protocols: 파일전달 프로파일, 헤드셋 프로파일 등과 같은 서비스 프로파일 관련 프로토콜이다.

3. 블루투스 프로토콜 분석기 설계

본 시스템은 펌웨어를 장착한 블루투스 디바이스가 윈도우 OS 환경하에서 비주얼 C 컴파일러를 구축한 PC에 UART나 USB로 접속되어 PC에서 소프트웨어로 블루투스 프로토콜 분석 기능을 수행하였다. 이들은 프로토콜 계층별로 처리하기 위해 블록으로 분류하여 모듈화하여 개발하였다. 블루투스 프로토콜 분석기는 펌웨어가 로딩된 디바이스와 UART나 USB로 접속되어 소프트웨어가 로딩된 PC로 구성된다. HCI 명령 송신 및 이벤트 수신, 데이타 패킷의 송, 수신을 모니터링하는 부분과 이들 패킷을 발생시켜 주는 시뮬레이션부분으로 구성되며, 송, 수신된 HCI 패킷을 user-friendly PC 화면에 디스플레이 하도록 한다. 이러한 프로토콜 분석은 계층화된 체계를 따라 HCI 프로토콜위에 L2CAP이 앤캡슐레이션되고, L2CAP 위에 SDP, RFCOMM, TCS가 앤캡슐레이션 된다. 또한 RFCOMM이나 TCS위에는 각종 블루투스 서비스를 위해 표준화된 프로파일이 존재한다. 따라서 블루투스 프로토콜 분석기는 프로토콜 스택부와 프로파일 부를 분류하고, 프로토콜 스택 부와 프로파일 부는 또 다시 시뮬레이션 기능에 따라 헥사 값을 사용자가 프로토콜 형태에 맞게 입력하는 매뉴얼 처리와 프로토콜 기능상 그 흐름을 처음부터 끝까지 동시에 처리하는 자동 처리등의 세부 항목으로 분류하여 PC 화면에 디스플레이 시킨다.

소프트웨어 설계는 구조와 기능의 편의상 블록으로 분류하여 처리하였는데, 설계된 소프트웨어를 사용자의 운용에 따라서 화면에 결과 값을 표현(display)하는 User/Interface 기능(여기서 편의상 소프트웨어 용어로 MMI 블록이라 함)으로 구분한다. 프로토콜 블록은 UART나 USB를 통하여 펌웨어와 송, 수신되는 HCI 프로토콜 데이타(L2CAP 등의 상위계층 프로토콜 데이타를 포함 할 수 있음)를 처리한다. MMI(Man Machine Interface) 블록은 프로토콜 블록으로부터 HCI 프로토콜 데이타의 시작주소와 정보의 내용을 포함하는 정보영역의 길이를 매개 파라메터로 하여 HCI 컨매드, 이벤트, 데이타 패킷이 펌웨어와 송, 수신 될 때마다 호출된다. 이렇게 호출된 MMI 블록은 사용자가 요구한 프로토콜 종류와 처리되어야 할 프로토콜 파라메터 등의 내용을 분석하여 펌웨어와 송, 수신된 프로토콜 정보를 사용자의 PC화면 출력 형태에 적합하게 디스플레이 한다. 즉, 프로토콜 분석기 관련 소프트웨어블록의 동작은 다음과 같다.

• MMI 블럭: 화면으로부터 입력되는 정보를 프로토콜 처리블록으로 사용자 요구에 맞게 처리하도록 하고, 프로토콜 처리블록으로부터 관련 정보를 수신하여 화면에 출력시킨다. 즉, 화면 출력 형태는 메시지마다 user-friendly하게 'HEXA', 'NEMONIC', '파라메터 서술부'의 조합으로 출력하여 초보자라도 프로토콜을 쉽게 이해 할 수 있도록 하였다. 특히 윈도우환경으로부터 입력되는 정보처리가 가능하도록 하고 실행파일은 프로토콜 내용의 디스프레이에 관련한 각종 메뉴를 정의하는 아이콘으로 구동되도록 하였다.

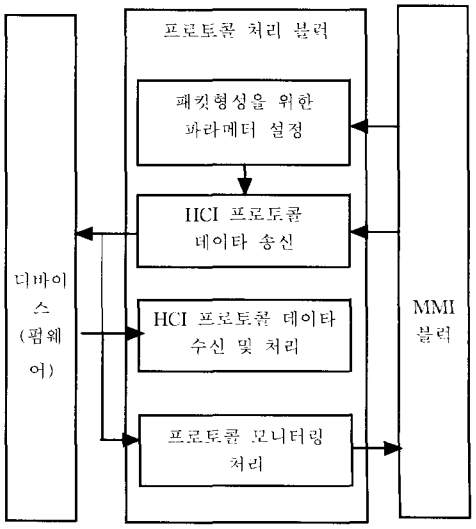

그림 2 프로토콜 분석기 처리 과정

• 프로토콜 처리블럭: 펌웨어와 블루투스 패킷의 송, 수신 처리에 관계되며, 펌웨어로 송, 수신된 HCI 패킷은 종류에 따라 HCI, L2CAP, RFCOMM, TCS, SDP 및 각종 프로파일별로 분류하여 MMI 블록에 전달하여 디스플레이를 요구한다. 블루투스 프로토콜 정보를 상대 시스템으로 송신하여야 할 경우는 프로토콜 정보형성과 전달이 필요하다. 이러한 정보 형성은 운용자가 요구한 프로토콜 종류와 그 내용(기본적으로 처리되어야 할 파라메터와 운용자 요구에 따른 패킷 선택별 파라메터 등)에 따라 처리된다. 즉, MMI블록을 통해 HCI, L2CAP, RFCOMM, TCS, SDP 등의 프로토콜별과 프로파일의 기능별로 패킷 발생을 수행하여 펌웨어로 송신한다. 이렇게 송신된 패킷은 프로토콜 처리 블록의 모니터링기능을 통해 MMI을 경유하여 user-friendly 하게 PC 화면에 디스플레이 된다.

4. 블루투스 프로토콜 분석기의 시험 및 특징

4.1 시험환경

본 시스템의 시험환경으로는 피코넷을 형성하여 블루투스 장비간 통신을 수행할 수 있으나 본 논문에서는 편리상 두 대의 블루투스 장비간 파일 전달과 블루투스 장비와 헤드셋간에 음성정보 전달을 수행하여 시험하였다. 본 시스템에서 하드웨어인 디바이스와 소프트웨어가 실장된 PC 간의 UART 통신의 속도는 다양하게 변화 가능하나 약 20kbps 이하의 속도를 제외하고는 성능에 영향을 거의 주지 않았으므로 한계치인 115kbps로 시험하였다. 파일 전달을 위해서는 두 개의 블루투스 시스템간 RFCOMM, L2CAP, HCI, SDP가 사용되고, 음성 전달을 위해서는 블루투스 시스템과 헤드셋간 시그널링으로는 HCI, L2CAP, SDP, TCS가 사용되고 음성 전달은 시스템내부에 존재한 PCM 코덱을 통해 전달됨으로 펌웨어만 사용된다.

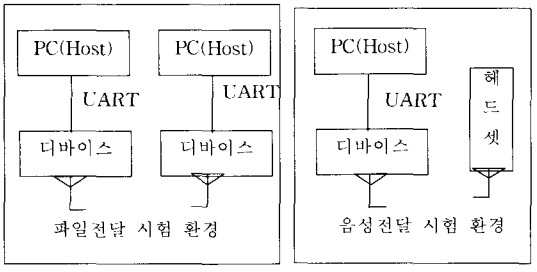

그림 3 시험환경

4.2 블루투스 프로토콜 분석기의 성능해석

블루투스 프로토콜 분석기 개발후 이의 성능을 파악하는 단계이다. 파일 전달을 위해 두 개의 블루투스 시스템간 RFCOMM, L2CAP, HCI, SDP를 통한 통신 처리량을, 음성 전달을 위해서는 블루투스 시스템과 헤드셋간 사용되는 HCI, L2CAP, SDP, TCS를 통한 호 처리 시간을 성능 분석 파라메터로 제시하였다.

4.2.1 파일전달시 성능해석

블루투스 시스템에서 한 개의 패킷을 형성하여 상대측 디바이스로 송신하는데 성능에 미치는 소요시간은 RFCOMM에서 파일 액세스 하는 주기적인 시간과 호스트와 디바이스에 연결된 UART 접속 환경이다. 파일 전달은 개발된 소프트웨어에서 파일 액세스 하는 주기적인 시간이 매우 큰 의미가 있었다. RFCOMM에서 액세스하는 파일의 패킷 크기는 가변이나 통상 많이 사용하는 128 바이트로 고정하고 시험 한 결과, 주기적인 파일 액세스 시간이 0.04초일 때 약 13kbps 처리량을 유지하는 블레이크 포인트 시간이었다. 즉, 파일 액세스 하는 시간이 0.04초보다 크면, 속도가 비례하여 처리량이 감소하고, 그 보다 적으면 동일한 처리량을 유지한 사실을 알 수 있었다.

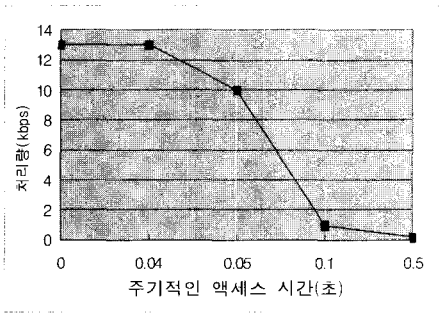

그림 4 파일 전달시 성능 분석 결과

4.2.2 음성전달을 위한 성능해석

음성 전달시 호 처리 성능 분석을 위해서 블루투스 시스템과 헤드셋간 사용되는 소프트웨어인 HCI, L2CAP, SDP, TCS를 통한 소프트웨어 처리 시간을 계산해 보면 다음과 같다.

시뮬레이션을 위해 한 개의 패킷을 형성하여 송신하는데 관련된 소요시간은 다음과 같다.

- 펌웨어 소요시간: 1ms
- 펌웨어와 소프트웨어간 프리미티브 호출 처리시간: 10ms(UART 전송시간 포함)

- 시뮬레이션 소프트웨어 처리시간: 0.1ms

시뮬레이션의 성능 분석은 정상적인 호 접속과 해제 관점에서 파악하였다. 정상적인 호 접속시, 송신측에서 송신하는 패킷은 SETUP, CONNECT_ACK 두 개이며, 수신하는 패킷은 CONNECT 한 개이다. 정상적인 호 해제시의 경우는 송신측에서 송신하는 패킷은 DISCONNECT, RELEASE_COMPLETE 두 개이며, 수신하는 패킷은 RELEASE 한 개이다. 따라서 정상적인 호 접속시 3개(2개 패킷 송신, 1개 패킷 수신)의 패킷과 해제시 3개(2개 패킷 송신, 1개 패킷 수신)의 패킷이 처리되며, 한 개의 호 접속과 해제시에는 약 66.6ms가 소요된다. 따라서 호 접속과 해제를 연속할 경우 초당 약 16번 처리할 수 있는 트래픽 능력을 처리할 수 있다.

4.3 블루투스 프로토콜 분석기의 특성

본 논문에서 제시된 프로토콜 분석기는 기존의 프로토콜 분석기[3]와 비교해 볼 때, 기존의 장비는 피코넷에서 발생하는 패킷의 모니터링 기능에 중점을 맞추었으나 본 논문에서 제시된 프로토콜 분석기는 블루투스 시스템 개발시 테스트 장비로 활용된다. 그림 5는 프로토콜 데이타 유닛 송, 수신시 그 정보를 PC 화면에 출력하는 형식을 나타내었다. 이와 같이 본 장비의 PC 화면 출력은 프로토콜 관련 파라메터의 헥사 값의 조합과 그 값의 의미 및 프로토콜/프로파일의 선택을 연관시켜 사용자가 쉽게 파악하도록 하였다.

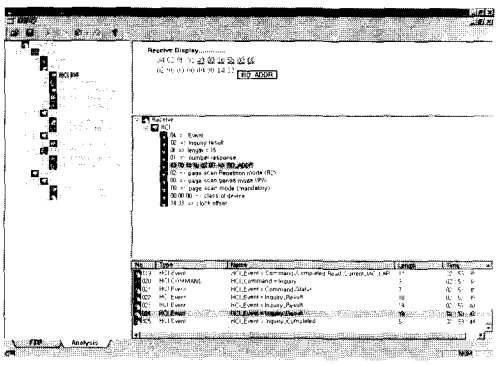

그림 5 송, 수신된 프로토콜 데이타 유닛

5. 결 론

본 논문에서는 블루투스 프로토콜 분석기 개발을 PC 기반 하에서 수행하였으며, 이의 동작과 기능을 제반환경과 더불어 살펴보았다.

프로토콜 분석기의 기능은 하드웨어인 블루투스 디바이스 위에서 펌웨어를 로딩하였으며, 디바이스와 UART 및 USB로 접속된 PC에 소프트웨어만 로딩하도록 하였다. 소프트웨어는 비주얼 C언어로 PC기반 하에서 윈도우를 운영체제로 사용함으로써 별도의 부가 장비 없이 손쉽게 프로토콜을 분석할 수 있는 환경을 구축하였으며, 추후 새로운 프로파일의 개발로 계속적인 프로파일 관련 프로토콜의 탑재가 가능하도록 개방된 구조로 설계하였다. 또한 설계된 시스템의 파일전달과 음성전달에 대한 성능도 분석하였다. 파일전달시 현재 개발된 시스템의 프로토콜 최대 처리 시간은 13kbps 정도임으로 블루투스 환경에서 장비 개발시 충분한 기능 검증용으로 활용될 수 있음을 입증하였다. 음성전달시 블루투스 호 설정과 해제 처리시간은 약 16.6ms이므로 초당 약 66개의 호 설정과 해제를 수행할 수 있음을 알 수 잇었다. 이와 같은 결과는 기저대역이 720kbps인 블루투스 통신을 고려하면, 관련 장비 개발시 충분한 성능 검증용으로 활용될 수 있다

향후에는 현재의 개발된 프로토콜 위주의 장비에서 기능적으로는 기존의 프로파일과 추후 권고될 프로파일의 개발을 추가하고, 외관적으로는 고속의 임베디드 환경에서 실현하여 완벽한 블루투스 프로토콜 분석기 개발이 요구된다.

참 고 문 헌

[1] Btent A Miller, "Bluetooth Revealed," Prentice-Hall, 2001.

[2] Bluetooth Special Interest Group, "Specification of Bluetooth System," Version 1.0B, http://www.bluetooth.com, 1999.

[3] Merlin, "Bluetooth Protocol Analyzer," http://www.catc.com, 1999.

[4] Bluetooth Test_Specs_4Jul01.zip Version 1.1, http://www.bluetooth.com, 1999.

[5] Jennifer Bray, "Bluetooth: Connect without Cables," Prentice-Hall, 2001.

정 중 수
1981년 2월 영남대학교 전자공학과(학사)
1983년 2월 연세대학교 전자공학과(석사)
1993년 8월 연세대학교 전자공학과(박사)
1983년 3월 ~ 1994년 2월 ETRI 연구원
선임연구원 1987년 8월 ~ 1989년 8월 벨지움 Alcal/Bell Telephone사 객원연구원
2000년 1월 ~ 2001년 1월 미국 UMASS/Lowell 전산학과 객원교수. 1994년 3월 ~ 현재 국립 안동대학교 공과대학 전자정보산업학부 부교수