

원거리 무선전송을 위한 DS-SS 모뎀 기반의 통신시스템 구현

Implementation of DS-SS Modem-based Communication System for Long Distance Wireless-Transmission

주원기*, 김윤호**, 이주신***

Won-Ki Ju*, Yoon-Ho Kim** and Joo-Shin Lee***

요 약

본 논문에서는 원거리 무선전송을 위한 DS-SS 기반의 통신시스템을 제안하였다. 설계된 모듈은 오류정정을 위한 길쌈부호와 T-DES 암호화를 사용하였고, 대역확산을 위해 골드코드 생성기를 적용하였다. 또한 모뎀의 검증과 인터페이스를 위한 FPGA/MCU 하드웨어와 데이터 송수신 동작과 같은 명령 신호를 제어할 수 있도록 PC 기반의 GUI 프로그램을 구현하였다. 설계된 하드웨어와 GUI 프로그램을 이용하여 전체 시스템의 동작을 검증하는 일련의 실험을 수행하였고, 실험결과 제안하는 통신시스템이 설계 규격대로 수행됨을 확인하였다.

Abstract

In this paper, we proposed the DS-SS modem-based communication system for long distance wireless-transmission. The module we designed in this approach contained both convolution encoder and gold-code generator, which aimed at error correcting, T-DES encryption algorithm and spread-spectrum as well. It embodied PC-based GUI program in order to control the such command signal as data transceiver. This program also used to control the specific FPGA/MCU which is able to verify and interface to the modem. We demonstrated the communication system to verify its proper operation by using GUI program and designed hardware. A set of experiments are conducted and as a result, proposed communication system is well operated as the design specification.

Key words : DS-SS, Modem, MCU, VHDL, Communication System

I. 서 론

최근의 무선 통신시스템은 고속화, 안정성이 뛰어난 기술이 적용된 최신 기술을 많이 사용하고 있지만 특수목적에 의해 CDMA나 DS-SS와 같은 시스템이 많은 부분에서 사용되고 있다. DS-SS 모뎀은 확산 코드를 이용하여 대역확산을 하므로 비화 특성이 우수

하고 방해파 억압 효과가 있으며[1], 일반적인 변조 방식과 달리 신호의 전력이 확산대역에 퍼져서 적은 양으로 균일하게 존재하여 신호 도용 확률이 적다. 또한 주파수 대역이 넓기 때문에 주파수 다이버시티 효과를 얻어 페이딩에 강하며[2], 다중 접속이 가능하기 때문에 특수 목적형으로 적합하다.

본 논문에서 제안하는 통신시스템은 원거리 전송

* 목원대학교 IT공학부 (Division of IT Engineering, Mokwon University)

** 목원대학교 컴퓨터공학부 (Division of Computer Engineering, Mokwon University)

*** 청주대학교 전자정보공학부 (Division of Electronic & Information, Cheongju University)

· 제1저자 (First Author) : 주원기,

· 교신저자 (Corresponding Author) : 김윤호

· 투고일자 : 2011년 12월 2일

· 심사(수정)일자 : 2011년 12월 2일 (수정일자 : 2011년 12월 27일)

· 게재일자 : 2011년 12월 30일

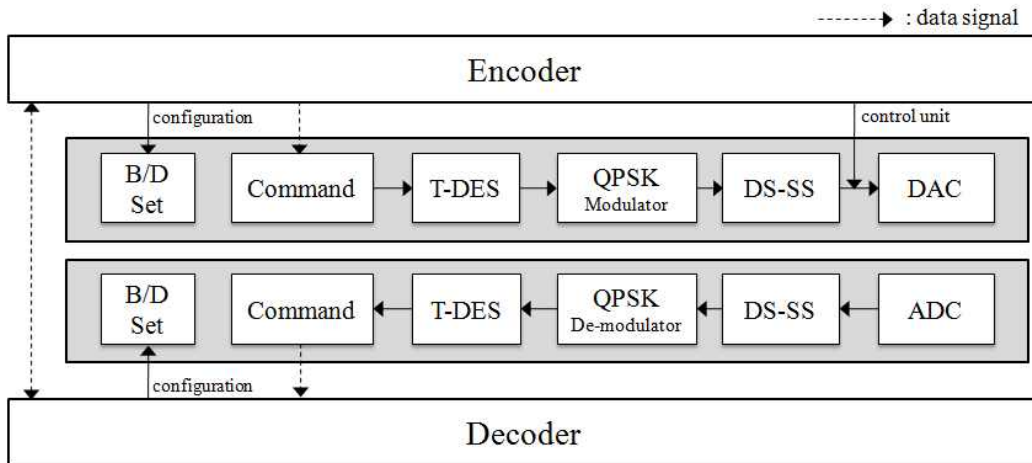


그림 1. 시스템 구성 블록도
Fig. 1. System structure block diagram

을 위한 DS-SS 기반의 모뎀으로 인코더와 디코더의 명령비화를 위하여 T-DES 보안 알고리즘을 적용하였고, 오류정정을 위하여 길쌈부호기를 사용하였다. 또한 변조는 QPSK 방식을 채택하였고, 골드코드(Gold code) 기반으로 코드 확산을 하였다. 인코더와 디코더 간의 통신은 ADC(Analog to Digital Converter)와 DAC(Digital to Analog Converter)를 사용하여 아날로그 기저신호 전송[3][4]으로 구현하였고, Tx와 Rx의 데이터를 검증하기 위해 DM(Diagnostic Monitoring) GUI를 설계하였다. 모뎀 설계는 MCU를 사용하여 GUI와 FPGA간 통신할 수 있는 구조로 B/D를 설계하였고, GUI를 통해 데이터통신을 검증하였다.

II. 제안하는 통신 시스템

그림 1은 제안 및 구현한 전체 시스템의 구성으로 명령비화 및 오류정정 인코딩은 각각 64비트 T-DES 알고리즘과 길쌈부호기를 사용하였으며, 코드확산은 골드코드 생성기를 적용하였다. 그림 2는 제안하는 시스템의 송신부로 데이터의 입력은 DM GUI에서 UART 통신으로 MCU에 전송하고, SPI를 통해 FPGA에 입력하는 구조로 설계되었다. 송신부는 T-DES, SFD, 길쌈부호기, DS-SS, QPSK 모듈로 구성된다.

T-DES 암호화는 DES의 brute-force 공격에 대한 취약성을 보완하기 위해 기존 DES 알고리즘을 반복적으로 적용하여 비닉성[5]에 강하다. 그림 3은 T-DES

의 암호화 및 복호화 과정으로, 64비트의 데이터와 키값을 입력으로 받아 각각 16-라운드 연산으로 암호화를 한다. 그림 3(a)와 같이 암호화 과정은 첫 번째와 세 번째 블록에서 암호화를 하고 두 번째 블록에서는 복호를 통해 이루어진다. 제안하는 시스템에서는 각 블록별 암호 키를 각각 지정할 수 있는 구조로 설계되었다.

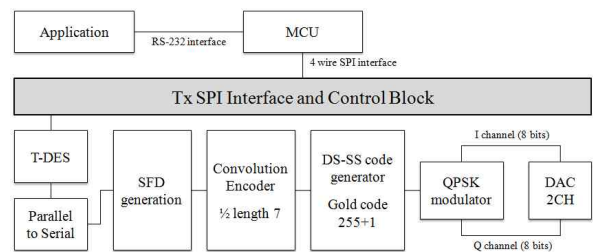


그림 2. DS-SS 모뎀 송신부
Fig. 2. DS-SS modem transmitter

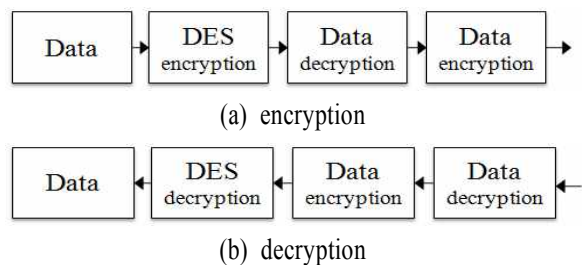


그림 3. T-DES 암호화/복호화
Fig. 3. T-DES encryption/decryption

그림 2에서 SFD(Start of Frame Delimiter)는 수신단의 프레임 동기를 잡기 위한 신호를 발생해 주는 블

죽으로 16비트로 구성되고, 코드확산[6][7]은 골드코드 생성기(38,400 chips of 255+1)를 적용하였다. 그림 4는 골드코드 생성기의 블록도이다.

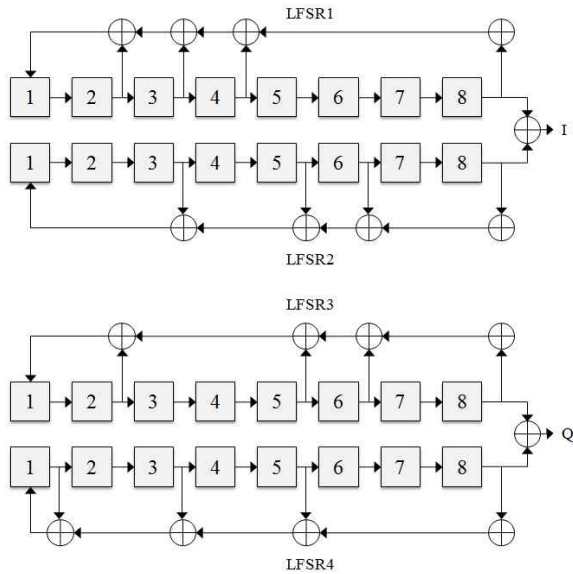


그림 4. 골드코드 생성기
Fig. 4. Gold-code generator

본 논문에서 오류정정 인코딩을 위해 부가성 백색 가우스 통로에서 오류정정 능력이 우수하고 연집에 러에 대한 정정능력을 높일 수 있는 길쌈부호기(그림 5)를 적용하였다 [8][9].

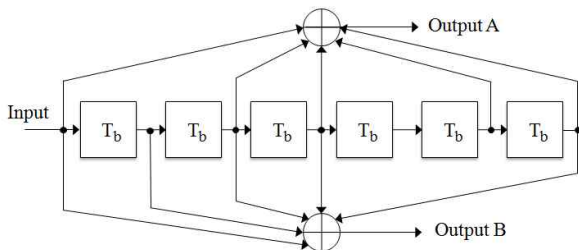


그림 5. 컨벌루션 부호기 블록도
Fig. 5. Convolution encoder block

본 논문에서 길쌈부호기에 의한 시스템의 성능해 석을 위해 부호율 및 구속장은 각각 1/2와 7이고 생 성다항식은 (171, 133)이며, 이에 대응되는 전달 함수 T(D, N)은 다음과 같다.

$$T(D) = 36D^{10} + 211D^{12} + 1,404D^{14} + 11,633D^{16} + 76,628D^{18} + 469,991D^{20} + \dots \quad (1)$$

$$\frac{\partial T(D, N)}{\partial N} = 33D^{12} + 28D^{14} + 2,179D^{16} + 15,035D^{18} + 105,166D^{20} + \dots \quad (2)$$

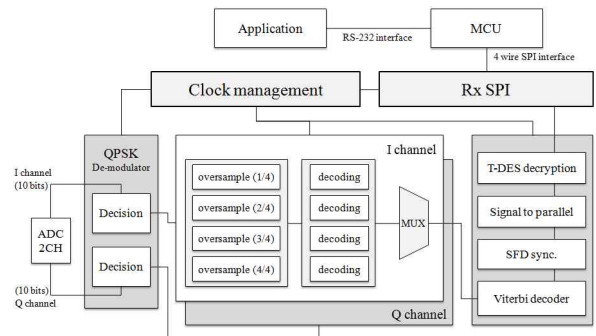


그림 6. DS-SS 모뎀 수신부
Fig. 6. DS-SS modem receiver

그림 6은 구현한 DS-SS 모뎀의 수신부로 주요블 록은 QPSK 디모듈, 역확산 블록, Viterbi 블록, 복호 화 및 SFD 싱크블록으로 구성되고, 송신부의 역관계 로 설계되었다 [10][11]. 결정블록에서 양자화된 데이 터를 디매핑하여 IQ로 변환되고 4X 오버샘플링되어 I와 Q 로 표현된다. 여기서 I와 Q는 각각 4비트로 표 현된다. 현재까지의 과정은 오버샘플링 클럭에 동기 되어 운용되고, 이후 디코딩 블록에서 다시 2비트로 표현된다. 디코딩 블록에서는 칩클럭에 동기되어 역 확산 동작을 하게 된다.

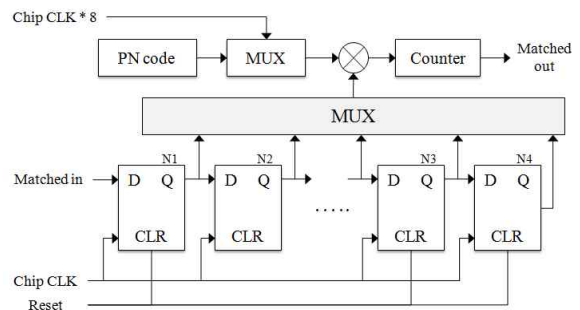


그림 7. 정합필터
Fig. 7. Matched filter

주파수 확산 방식에서는 능동상관기에 의한 동기 획득 방식 또는 정합필터를 사용하여 동기를 획득하게 되는데, 능동상관기 구조의 경우에는 동기 획득의 결정을 위해 연산값을 누적해야 하며 이는 빠른 동기 획득에 있어 매우 비효율적인 방법이다. 본 논문에서는 능동상관기의 이러한 단점을 보완하기 위해 정합필터(그림 7)를 기본 모델로 선택하였다.

역확산 블록에서는 초기 데이터 결정을 거쳐 오버샘플링한 I와 Q를 각각 디코딩한다. 또한 데이터 결정 블록에서는 ADC에서 입력받는 초기 데이터를 QPSK 디맵핑[12] 연산을 통해 2진 데이터로 표현된다. I와 Q채널은 각각 4개로 구성되며 오버샘플링 블록에서 1/4chip 단위로 서로 다른 위상의 값을 넘겨주어 역확산 동작을 한다.

또한 비터비복호기[13][14]는 그림 8과 같으며 BM(Branch Metric), ACS(Add Compare Select), 역추적(Trace Back), LIFO(Last In First Out) 및 제어부로 구성된다.

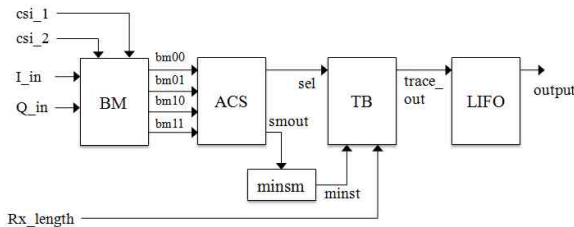


그림 8. 비터비복호기
Fig. 8. Viterbi decoder

본 논문에서 구현된 비터비복호기는 길쌈 부호기에 대한 복호를 수행하며, 해밍거리에 의한 연성 판정을 적용하였고 복호길이는 48이다. 역추적부는 고속의 데이터를 처리하기 위해 8개의 메모리 뱅크를 사용한 3포인트 알고리즘을 적용하였다. 각 메모리는 복호길이의 절반인 24개의 주소를 가지며 각 주소별로 64비트의 길이를 가진다. 또한 역추적을 위해 3 포인트 알고리즘을 적용하였기 때문에 TB부에는 역추적을 위한 모듈이 3개 사용된다. 상기 3개의 역추적 모듈 중 2개는 역추적을 수행하고 하나는 복호과정을 교대로 수행하게 된다. 3개의 역추적 모듈 중 복호를 담당하는 것은 하나의 모듈로써 이는 제어신호에 의해 선택된다. 수신부의 마지막 단계인 T-DES 블록에서는 그림 3(b)의 과정을 통해 이루어진다.

III. DM GUI 구현 및 검증

검증 시스템은 크게 세 부분으로 Tx 모듈/펌웨어, Rx 모듈/펌웨어, PC 기반의 GUI로 구성된다. GUI 프로그램에서는 Tx/Rx 모듈에 데이터 전송 요청, 수신된 데이터 확인, DES 키 설정 및 알림, ID 설정 등의 기능을 갖는다. 그림 9는 시스템의 전체 데이터 흐름을 나타내고 있다. MCU에 내어저장되고 동작되는 Tx/Rx 펌웨어는 GUI와 FPGA간 인터페이스 역할을 담당한다.

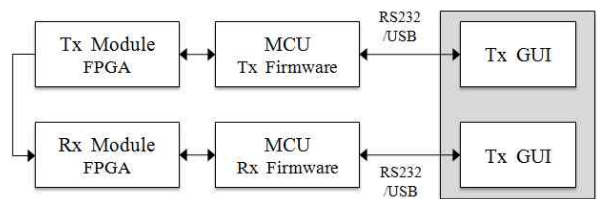


그림 9. 시스템 흐름도
Fig. 9. System flow

3-1 Tx와 Rx 모듈

그림 10은 Tx 모듈의 데이터 흐름도이다. GUI와 MCU 간의 RS232통신을 위해 COM 포트를 개방하고,

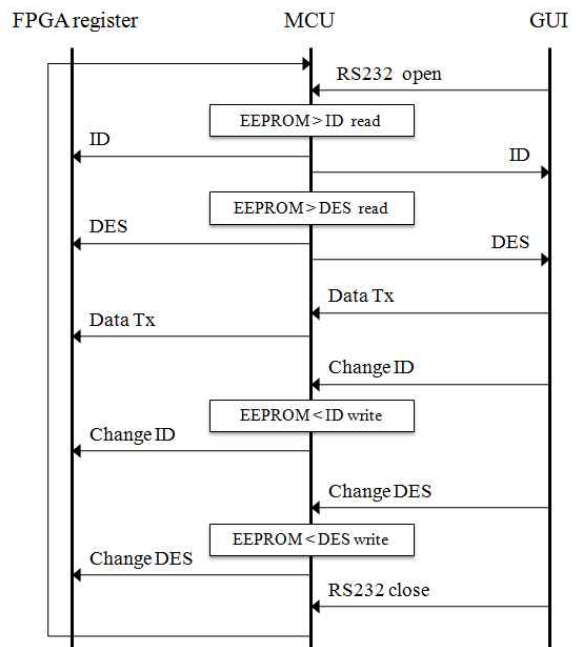


그림 10. Tx 데이터 흐름도
Fig. 10. Tx data flow

MCU 내부에 존재하는 EEPROM에서 마지막 저장된 ID와 DES 키 값들을 FPGA 데이터 프레임 레지스터와 DES 레지스터들에 적재한다. FPGA와 GUI 초기 세팅이 마무리되면 MCU는 GUI에서 전달된 메시지들을 대기시키다. 이 시점부터 받을 수 있는 메시지는 데이터 전송 요구 메시지, ID값 변경 요구 메시지, DES1/2/3에 대한 각각의 변경 메시지이다.

마지막으로 RS232 폐쇄 메시지를 입력되면 RS232가 개방될 때 까지 대기한다. 주 동작은 데이터 전송 메시지이며 MCU는 이 메시지를 받는 즉시 FPGA에게 데이터 전송을 요구하게 된다. Rx 모듈안의 MCU에서 동작되는 펌웨어는 Tx 모듈내 펌웨어와 동일하게 GUI와 FPGA 사이의 데이터 전달 역할을 한다.

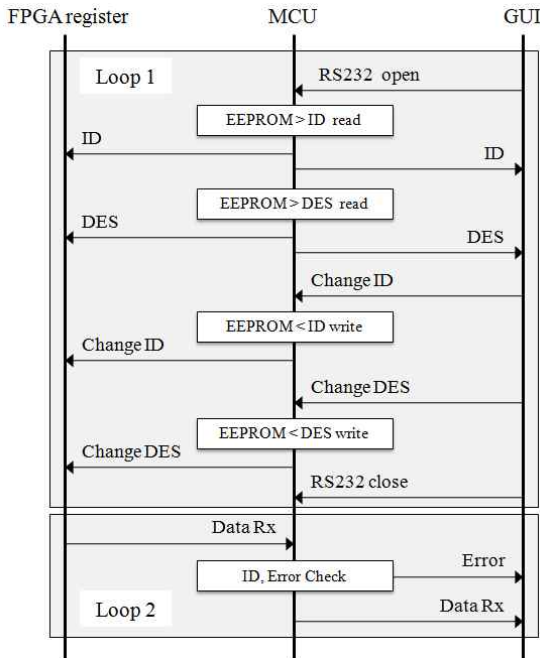


그림 11. Rx 데이터 흐름도
Fig. 11. Rx data flow

수신부 모듈 내 MCU 펌웨어가 시작되면 루프 1이 동작되어 FPGA와 GUI 초기 세팅이 마무리되면 루프 2에서 수신동작을 연속적으로 진행할 수 있게 된다. GUI에서 메시지가 전달되면 다시 루프 1내로 진입하여 메시지를 처리하고 루프 2로 돌아와 수신동작을 한다. 주 동작은 데이터수신이며, MCU는 수신부 FPGA로부터 수신데이터가 도착하면 바로 GUI로 ID 및 Error 체크, 그리고 수신 데이터를 메시지 형태로 보낸다.

3-2 DM 프로그램

Tx 모듈과 Rx 모듈의 데이터 전송 및 수신 동작을 PC 기반의 GUI 프로그램으로 제어하고, ID 및 DES 키값의 설정, 버튼 방식의 명령 설정이 가능하도록 DM(Diagnostic Monitoring) 프로그램을 구현하였다. 또한 에러의 요율을 계산하는 기능을 구현하여 효율적인 검증이 가능하도록 하였다. GUI와 장비간에는 Tx 모듈과 Rx 모듈에 각각 USB 케이블로 연결하여 RS232 통신으로 필요한 메시지를 수수한다. Tx GUI와 Rx GUI는 각각의 RS232 포트를 통해 각 모듈과 연결되어 개별적인 메시지 송수신 라인을 형성한다.

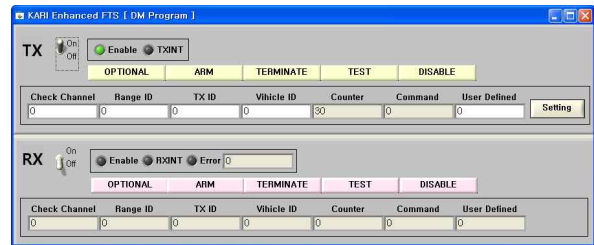


그림 12. DM 프로그램
Fig. 12. DM program

3-3 실험결과

본 논문의 Modem 블록과 인터페이스 블록은 실시간으로 처리가 용이하고 소자의 제약이 적게 하기 위해 주요 알고리즘을 모두 VHDL로 설계하였으며 설계된 알고리즘의 성능검증에 초점을 두고 실험을 수행하였다.

시뮬레이션 수행 결과, 오버플로우가 나지 않는 한 디코더에서 하나의 프레임도 놓치지 않고 수신하고 있는 것을 확인하였고 T-DES 암호기법의 성능검증을 위해 송수신부의 암호키를 변경하면서 실험을 수행하였으며 오류보정기법의 알고리즘을 검증하기 위해 인위적으로 복원 가능한 범위 내의 오류비트를 삽입하여 실험을 수행한 결과 모두 정상적으로 동작하는 것을 확인하였다.

그림 13과 그림 14는 각각 Tx와 Rx의 PnR(Place & Route)후 시뮬레이션 결과를 나타내고 있다.



그림 13. Post PnR 시뮬레이션 파형(encoder)
Fig. 13. Post PnR simulation wave(encoder)

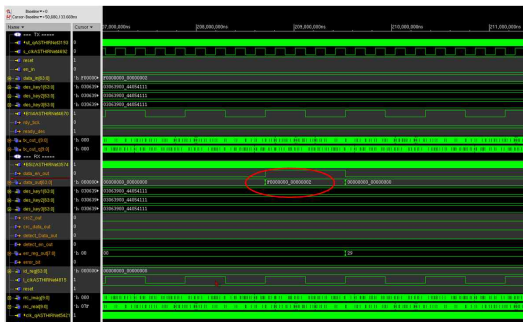


그림 14. Post PnR 시뮬레이션 파형(decoder)
Fig. 14. Post PnR simulation wave(decoder)

설계된 Modem의 인코더와 디코더 VHDL코드는 그림15와 같이 실제로 제작된 하드웨어에 탑재되어 그 기능을 확인하였으며 3-3에서 설명한 DM 프로그램을 사용하여 효율적인 기능 점검을 수행 하였다.



그림 15. 프로토타입 하드웨어
Fig. 15. Prototype hardware

IV. 결 론

본 논문에서는 DS-SS 방식의 통신시스템을 하드

웨어로 구현하기 위한 알고리즘의 이론적인 검토와 모듈별 설계에 관한 연구를 수행하였다.

MCU와 LABVIEW를 사용해 검증 프로그램을 설계하여 모뎀뿐만 아니라 통신시스템 전체의 검증을 할 수 있도록 설계하여 동작을 검증하였다. 모뎀 프로세서는 주파수 효율성이 좋고, 주변 신호에 의한 간섭에 강하며, 비밀유지에 효과적인 대역확산 방식을 이용하였으며 신호 검파는 차동 엔코더/디코더 방법을 사용하였다.

모뎀의 송수신부를 구현하기 위한 알고리즘을 바탕으로 VHDL로 모뎀 프로세서를 모듈별로 구현하여 Altera사의 EP2S30를 대상 소자로 설계한 결과 약 25%의 리소스가 사용되었고, 설계 검증을 위해 프로토타입의 FPGA/MCU 보드도 실제 구현하여 실험을 완료하였다. 시뮬레이션을 통하여 동작에 이상이 없음을 확인한 후 FPGA/MCU 보드와 DM 프로그램 기반으로 그 기능을 검증하였다.

본 연구에서는 한정된 기능의 모뎀을 설계하였지만 향후에 다양한 채널코딩 기법과 Test Vector를 추가하여 비교 검증할 수 있는 DM 프로그램을 개발하고자 한다.

참 고 문 헌

- [1] Jung-Ha Lee, Il-Hwan Kim, "Design of a Wireless Modem Processor Using Direct Sequence Spread Spectrum Communication Method", *Journal of Telecommunications and Information*, Vol. 8, pp.21-25, 2004.
- [2] Shimon Moshavi, Bellcore, "Multi-user detection for DS-CDMA communications" *IEEE Communication Magazine*. pp 137-146 October 1996.
- [3] 황태준 외, "무선 환경 노드의 핸드오버 알고리즘에 관한 연구", *한국정보기술학회 논문지 제 9 권 제 5 호*, pp.193-200, 5. 2011.
- [4] 이희종 외, "주파수-전압 변환 방식 스펙트럼 센싱을 이용한 채널 선택적 RF시스템", *한국정보기술학회 논문지 제 9 권 제 2 호*, pp.77-84, 2. 2011.
- [5] 권도윤 외, "Triple DES 알고리즘을 이용한 디지털

콘텐츠 보호 시스템 설계 및 구현”, *한국콘텐츠학회 논문집*, 제1권 제 1호, pp.160-164, 2003

- [6] 임금상 외, “대역확산방식 비행종단시스템의 모델 설계와 구현에 관한 연구”, *한국통신학회논문지 제 31권 제2호*, pp.175-183, 2. 2006.
- [7] 원희석 외, “대중저속 무선 통신을 위한 DSSS 모델 설계 및 구현”, *전자공학회 논문지 제 43권 TC 편*, 제1호, pp.121-126, 1. 2006.
- [8] Savo Glisic, Branka Vucetic, “Spread Spectrum CDMA systems for wireless communications”, *Artech House Publishers*, April 1997.
- [9] John G. Proakis. “Digital Communications”, Prentice Hall. pp. 729-734, 2000.
- [10] W. Hang et al., “Performance of DSSS against repeater jamming,” *Proc. ICECS*, pp. 858-861, Dec. 2006.
- [11] J. Jindapun and R. Suleesathira, “Blind adaptive LMS beamforming using projection technique in DSSS system,” *International workshop on Advanced Image Technology*, pp. 473-477, Jan 2006.
- [12] P.D. Cho and B.G.Kang, “Design and Implementaion of QCQPSK/HPSK Modem using Digital Signal Processors for Software Defined Radio Applications” in *Proc. of IEEK Conf.*, pp. 1428-1431, July 2002.
- [13] C. Cheng and K.K. Parhi, “Hardware Efficient Low-latency Architecture for High Throughput Rate Viterbi Decoders,” *IEEE Trans. on Circuits and Systems*, pp. 1254-1258, Dec 2008.
- [14] Qing Li, Xuan-zhong Li, Han-hong Jiang and Wen-hao He, “A High-speed Viterbi Decoder,” *IEEE Fourth International Conference on Natural Computation*, pp. 313-316, Oct 2008.

주 원 기 (朱元基)



2004년 2월 :목원대학교
컴퓨터공학과 공학사.
2007년 2월 :순천대학교 공학석사
2008년 4월~2010년 10월 :
(주)이니솔루션 대표이사.
2009년 3월~현재 : 목원대학교
IT공학부 박사과정.

관심분야 : SoC, FPGA, Modem 등

김 윤 호 (金允鎬)



2003 - 현재: 목원대학교 컴퓨터공
학부 교수
2005-2006: University of Auckland.
NZ, CITR Lab Research Fellow
2008-현재: ISO/TC223 Korea
Delegate

IEEE, 대한전자공학회,
한국통신학회 정회원/ 한국디지털컨텐츠학회,
한국항행학회, 사회안전학회 종신회원 / 멀티미디어
기술사.

관심분야 : 영상처리, 컴퓨터비전, 사회안전 및 IT정책,
방재정보통신 등.

이 주 신 (李周信)



1975년 : 명지대학교 전자공학과
공학사.
1977년 : 홍익대학교 전자공학과
공학석사.
1986년 : 명지대학교 전자공학과
공학박사.
1979.9~현재. 청주대학교

전자정보공학부 교수.

관심분야 : 영상처리, 디지털 신호처리, 컴퓨터비전 등.