

대역확산방식 비행종단시스템의 모뎀설계와 구현에 관한 연구

준회원 임금상*, 김재환*, 정회원 조항덕**, 김우식*

A Study on the Design and Implementation of a DSSS-based MODEM for a Flight Termination System(FTS)

Keumsang Lim*, Jaehwan Kim* *Associate Members*,
Hyangduck Cho**, Wooshik Kim* *Regular Members*

요 약

본 논문에서는 주파수대역 직접확산방식(DS-SS)의 비행종단시스템을 제안하였고 FPGA를 이용하여 구현된 결과를 보여준다. DS-SS방식의 비행종단시스템은 간섭신호와 jamming에 강한 특성이 있을 뿐만 아니라 확산코드를 사용함으로써 인증과 암호화의 효과를 얻을 수 있다. 또한 기존의 아날로그 FM방식의 종단시스템에 비하여 전력을 크게 줄일 수 있다. 오류정정을 위하여 리드-솔로몬(32, 28)코드를 적용하였고 데이터를 암호화하기 위하여 3중 Data Encryption Standard (3DES)암호화를 하였다. 그리고 counter알고리즘을 적용하여 외부 장치의 간섭으로부터 비행체를 보호할 수 있도록 하였다. I채널과 Q채널의 확산코드는 GOLD코드생성기를 이용하여 생성하였다. 시스템은 ALTERA EPXA1F484C3 디바이스로 지상시스템을 구현하였고, FLEX계열인 EPF10K100ARC240 디바이스를 사용하여 비행종단 탑재시스템을 구현하였다.

Key Words : FTS, Authentication, DS-SS

ABSTRACT

This letter proposes a Direct Sequence Spread Spectrum (DS-SS)-based Flight Termination System(FTS) and show the simulation results and implements the system using FPGAs. The DS-SS FTS has immunity to interference signals and the influence of jamming signal. Moreover, a DS-SS FTS can provides effects on an authentication and encryption with spread codes. And the system uses more less power than an analog FM system. We used Reed-Solomon (32, 28) code and triple Data Encryption Standard(3DES) for error correction and data encryption. Also we used counter algorithm for unauthenticated device's attack The spread codes of In-phase channel and Quadrature channel were generated by Gold sequence generators. The system was implemented in Altera APEX20K100E FPGA for the ground system and EPF10K100ARC240-3 for the airborne system.

I. 서 론

비행종단시스템이란 비행체가 발사된 후 여러 가

지 요인들로 인하여 비행영역을 벗어나거나 비행체의 추적이 불가능한 경우, 통신링크의 단절로 인하여 비행체와의 통신이 불가능한 경우 지상의 통제

※ 본 연구는 KOSEF, ABRC와 UBDC의 지원으로 수행되었습니다.

* 세종대학교 정보통신공학과 통신용신호처리 연구실 (jpeace, ssmiless}@sju.ac.kr, wskim@sejong.ac.kr),

** NVH Lab, Autosys Co.,Ltd (whiteblack@paran.com)

논문번호 : KICS2005-09-361, 접수일자 : 2005년 9월 1일

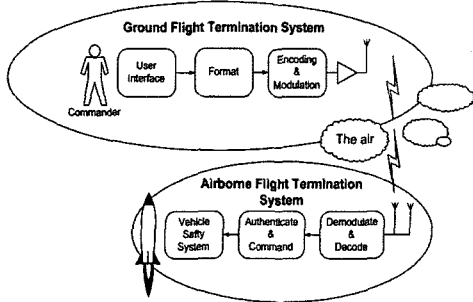


그림 1. 일반적인 비행중단시스템의 기본구성

시스템에 의하여 비행을 중단시키는 시스템을 말한다. 따라서 비행중단시스템의 모뎀기능은 통신모뎀의 성능보다 더 우수해야 하고 높은 신뢰성과 안정성이 요구되며 비행체내의 다른 시스템과 독립성이 보장되어야 하는 등 시스템요구사항이 매우 까다롭다^[1].

비행중단시스템의 변조방식으로는 High Alphabet (HA), Continuous Phase Frequency Shift Keying (CPFSK), Code Division Multiple Access(CDMA) 방식 등이 있으며, 본 논문에서는 주파수확산방식의 비행중단시스템을 제안하였다. 본 논문의 구성은 II장에서 일반적인 비행중단시스템에 관하여 설명하고, III장에서는 설계한 DS-SS방식의 FTS에 대해서 설명한다. 그리고 IV장에서는 시뮬레이션 결과를 보였고, 마지막으로 V장에서 결론을 맺는다.

II. 일반적인 비행중단시스템

비행중단시스템은 지상에서 발사체에게 명령을 전송하고 발사체의 상태를 모니터링 하는 Ground Flight Termination System(GFTS)과 발사체 전자탑재부에 탑재되는 Airborne Flight Termination System(AFTS)으로 구성된다.^[1] 그림 1은 비행중단시스템의 기본적인 구성도를 보여준다. GFTS에는 커맨더의 명령을 입력받는 User Interface와 명령을 FTS 형식에 맞게 변형시켜주는 Formatter, 그리고 암호화와 채널부호기, MODEM변조부등으로 구성된다. AFTS는 안테나로부터 수신되는 RF신호를 복조하는 MODEM복조부와 채널복호기, 암호복호기, 그리고 복호된 메시지를 인증할 수 있는 인증 메커니즘과 폭파 장치 등으로 구성된다.

2.1 Ground System

일반적인 GFTS는 시스템의 안정성을 보장하기 위하여 그림 2에서 보는 것과 같이 2중 설계구조로

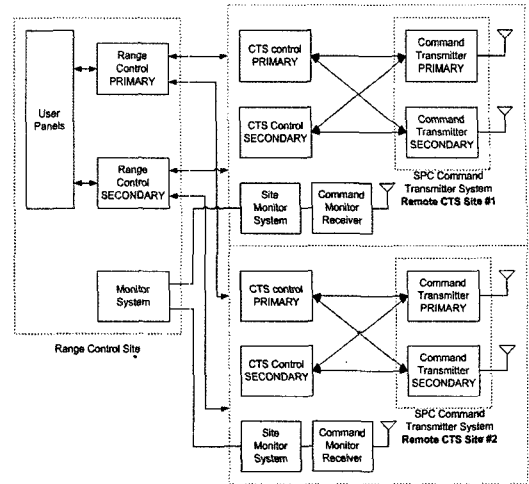


그림 2. 일반적인 GFTS 시스템

구성된다. User Panel로부터 입력받은 명령은 두 개의 Range Control Unit으로 입력되고 이것은 각각 원격지의 CTS에게 전송되어 최종적으로 두개의 Command Transmitter에 의해 비행체에게 전송된다.

2.2 Airborne System

AFTS는 발사체의 내부에 탑재되는 시스템으로 안전성을 보장하기 위하여 Ground System과 같이 2중으로 설계된다. 그림 3은 일반적으로 전술미사일 등에 사용되는 전형적인 AFTS의 수신시스템이다. 2개의 UHF안테나를 통하여 수신된 신호를 RF coupler를 통하여 각각의 CRD로 입력시킨다. CRD로부터 판독된 명령은 Safety Device를 통하여 명령의 유효성을 판단하고 명령이 유효하면 최종 구동부로 명령이 전달된다. 구동부는 해당 비행체에 적절한 파괴위력을 갖는 물리적 기폭장치와 그 제어장치로 구성되어 있다.

III. DS-SS방식의 FTS

3.1 DS-SS FTS Ground System

제안하는 DS-SS방식의 GFTS는 32bit Microprocessor Core, 암호화모듈, 오류정정코드 인코더, 차분인코더, Pseudo Noise code생성기, 그리고 마지막으로 변조부로 구성된다. Microprocessor Core는 ARM사의 32bit Microprocessor인 ARM922T Core를 사용하였다. ARM Core는 ARM사의 대표적인 processor로써 현재 가장 널리 사용되고 있는 프로세서이기 때문에 안정성과 신뢰성은 이미 입증되어 있다.

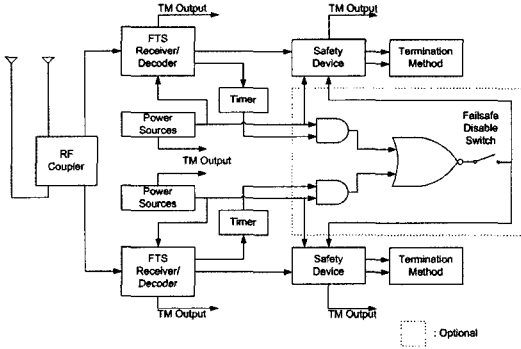


그림 3. 일반적인 AFTS 시스템

GFTS의 메시지처리 process는 다음과 같다. Micro-processor는 외부로 부터 입력되는 신호를 인터럽트 신호로 입력받아 Display Device를 통하여 현재 상태를 표시하여 주고 Frame Formatter는 커맨더로부터 받은 외부입력신호를 중단명령형식으로 변환해주는 일종의 인코더로서 명령스위치를 통하여 명령을 입력받으면 입력받은 신호에 따라 해당하는 명령으로 Frame Formatting을 한다. Frame Formatting된 메시지는 외부의 인증되지 않은 장치들로부터 데이터를 보호하기 위하여 암호화과정을 거치는데 DS-SS방식의 비행중단시스템에서 사용된 암호화방식은 2개의 Key를 갖는 Triple-DES를 사용하였다. Key의 길이는 128bit길이의 Key를 사용하였고 하드웨어의 크기를 줄이기 위하여 M. McLoone이 제안한 Key 스케줄링기법을 이용하여 구현하였다^{2, 3)}. Triple-DES processor에 의하여 암호화된 메시지들은 Reed-Solomon Encoder에 의하여 인코딩된다. Reed-Solomon 인코딩과정을 거친 메시지는 QPSK 변조를 하기 위하여 Serial to Parallel(S/P)모듈에 의하여 I-channel과 Q-channel로 분리되어 Differential Encoder의 입력으로 전달된다. S/P의 입력을 $x(n)$ 라 할 때, 출력 $I(t)$ 와 $Q(t)$ 는 다음과 같이 나타내어 질 수 있다.

$$I(t) = \sum_{n=0}^{k-1} x(2n), k = \text{frame size} \quad (1)$$

$$Q(t) = \sum_{n=0}^{k-1} x(2n+1), k = \text{frame size} \quad (2)$$

그리고 $I(t)$ 와 $Q(t)$ 는 각각 Differential Encoder의 입력으로 들어간다. 이 중에 $I(t)$ 의 경우만 봤을 때 Differential Encoder의 출력 $d(t)$ 는

$$d(t_0) = I(t_0) \text{ XOR Initial value} \quad (3)$$

$$d(t_k) = I(t_{k-1}) \text{ XOR } I(t_k), k > 0 \quad (4)$$

와 같이 나타내어진다. 비행중단시스템과 같이 송수신기가 물리적으로 따로 떨어져 있을 경우 전기적으로 기준이 되는 Ground가 서로 다를 수 있다. 다시 말하면 송신기와 수신기간의 전압기준이 다를 수 있다는 의미인데, 송수신기간의 기준전압레벨의 차이는 수신기에서 노이즈로 나타날 수 있다. Differential Encoding은 이미 이전에 수신된 신호가 기준이 되므로 이와 같이 물리적으로 분리된 송수신기 사이에는 Differential Encoding이 효과적이다. 그러나 같은 성능의 Bit Error Rate(BER)가 요구될 때 QPSK 변조보다 DQPSK 변조의 E_b/N_0 가 약 3dB 정도 더 요구된다.

Differential Encoder에 의해 Encoding과정을 거친 신호는 PN-code Generator로부터 생성된 PN-code를 이용하여 확산된다. PN-code Generator로부터 생성된 PN-code를 $c(t)$ 라고 가정하고 $d(t)$ 를 구형파형식으로 다시 표현하면

$$d(t) = \sum_{n=0}^{k-1} a_n I(t - nT_b) \quad (5)$$

$a_n = \pm 1, k = \text{frame size}$

$$c(t) = \sum_{n=0}^{m-1} c_n p(t - nT_c) \quad (6)$$

$c_n = \pm 1, m = \text{PNcode size}$

$$u(t) = d(t)c(t) \quad (7)$$

와 같이 나타낼 수 있다. 여기서 T_b 는 한 bit의 길이를 말하며 $p(t)$ 는 주기가 T_c 인 펄스신호를 말하고 보통 하나의 chip이라고도 한다.

$$g1(x) = 1 + x^2 + x^3 + x^4 + x^8 \quad (8)$$

$$g2(x) = 1 + x^3 + x^5 + x^6 + x^8 \quad (9)$$

$$g3(x) = 1 + x^2 + x^5 + x^6 + x^8 \quad (10)$$

$$g4(x) = 1 + x + x^3 + x^5 + x^8 \quad (11)$$

식 8부터 11까지는 DS-SS방식의 FTS를 위해 설계한 Gold code generator 각각의 생성다항식을 나타내었다. 그림 4는 8-stage의 Gold code generator의 블록다이어그램을 보여준다. 그림에서 보는 것과 같이 Gold code generator는 두개의 M-sequence generator출력을 서로 XOR하여 code를 생성한다.

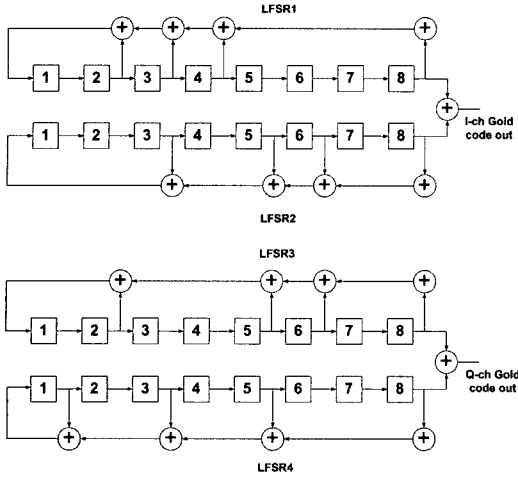


그림 4. 8-stage Gold code generator의 블록다이어그램

3.2 DS-SS FTS Airborne System

GFTS에서 전송된 명령은 RF회로에 의하여 전기 신호로 변환되고 다시 ADC를 통하여 Digital신호로 변환된다. 변환된 Digital신호는 carrier신호를 제거하기 위하여 수신기의 DDFS에서 생성된 신호와 함께 Complex Multiplier를 통하여 Down Conversion 된다. 이때 사용된 DDFS는 GFTS에서 사용한 것과 같은 성능의 주파수합성기이다. 송신기에서 전송된 신호를 TxOUT(t)이라고 한다면 TxOUT(t)는 아래와 같이 나타낼 수 있다.

$$TxOUT(t) = S_I(t)\cos(ut) + S_Q(t)\sin(ut) \quad (12)$$

그리고 정보신호의 위상과 국부반송파를 분리하기 위한 수식은 다음과 같다. 수신기에서 수신된 신호를 RxIN(t)라고 하고 Complex Multiplier의 입력을 I_{in}, Q_{in}, 출력을 I_d, Q_d라고 한다면 입력과 출력의 관계는 식 (14)와 식 (15)의 관계가 성립된다.

$$RxIN(t) = I_{\in}(t) + jQ_{\in}(t) \quad (13)$$

$$\begin{aligned} I_d(t) &= I_{\in}(t)\cos(ut) - Q_{\in}(t)\sin(ut) \\ &= [I_C(t)\cos(ut - \varphi) + Q_C(t)\sin(ut - \varphi)]\cos(ut) \\ &\quad - [Q_C(t)\cos(ut - \varphi) - I_C(t)\sin(ut - \varphi)]\sin(ut) \\ &= I_C(t)\cos\varphi - Q_C(t)\sin\varphi \end{aligned} \quad (14)$$

$$\begin{aligned} Q_d(t) &= I_{\in}(t)\sin(ut) + Q_{\in}(t)\cos(ut) \\ &= [I_C(t)\cos(ut - \varphi) + Q_C(t)\sin(ut - \varphi)]\sin(ut) \\ &\quad + [Q_C(t)\cos(ut - \varphi) - I_C(t)\sin(ut - \varphi)]\cos(ut) \\ &= I_C(t)\sin\varphi + Q_C(t)\cos\varphi \end{aligned} \quad (15)$$

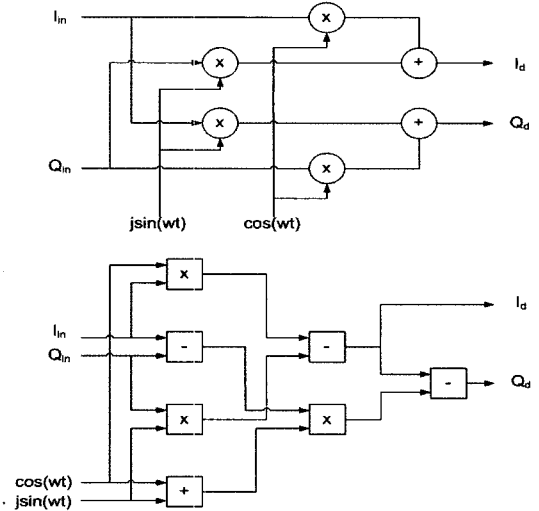


그림 5. Complex Multiplier의 블록다이어그램과 Micro-Architecture

그림 5는 Complex Multiplier의 블록다이어그램과 Micro-Architecture를 보여준다. 그림에서 보는 것과 같이 Complex Multiplier는 3개의 곱셈기와 4개의 덧셈-뺄셈기로 구현이 가능하다. Complex Multiplier의 cosine과 sine입력은 DDFS를 통해서 입력받는다.

Carrier신호가 제거된 데이터는 이진데이터인 0과 1로 변환하기 위하여 Integrate and Dump Filter를 이용하여 적분을 한다. Filter의 입력과 내부의 Dump register에 누적되어 있던 값이 더해져 출력되고 이 값은 임계값 비교기를 통하여 '0' 또는 '1'의 이진 데이터로 판별된다. 그림 6은 Integrate and Dump Filter의 출력파형을 보여주고 있다.

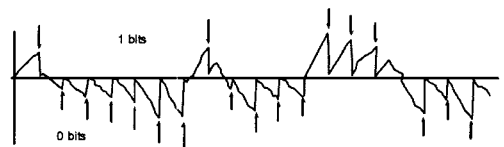


그림 6. Integrate and Dump filter의 출력파형

임계값 비교기를 통하여 이진 신호로 변환된 데이터는 PN-code의 동기 획득을 위하여 상관기의 입력으로 들어간다. PN-code 동기 알고리즘으로는 능동 상관기와 Matched Filter방식이 있다. 능동 상관기는 하나의 PN-code 위상에 대한 동기 획득 여부를 판단하기 위해서는 적분시간 동안의 탐색시간이 필요하게 되는데 이 탐색시간은 PN-code의 빠른 동

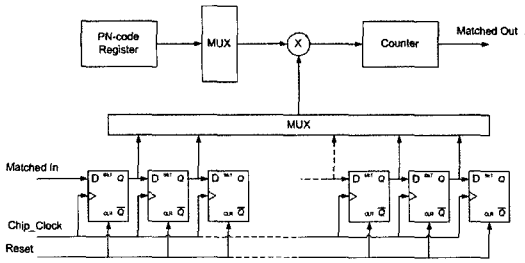


그림 7. Matched Filter의 블록 다이어그램

기 획득에 매우 큰 걸림돌이 된다. Matched Filter는 적분시간이 오래 걸리는 능동 상관기의 단점을 보완하기 위해서 제안된 방식이다. Matched Filter는 일정기간동안 수신된 신호와 PN-code를 곱한 값을 누적하는 부분이 없다. 따라서 비행중단시스템과 같은 긴박한 시기에 빠른 응답시간을 요구하는 시스템에 적합하다. 그러나 Sum of Product회로에 의한 하드웨어 크기의 부담이 증가하는 부작용도 있지만 FTS는 하드웨어 크기에 대한 제약이 휴대용 단말기 등에 비하여 비교적 적기 때문에 응답속도 면에서 성능이 우수한 Matched Filter방식을 적용하기로 하였다. 그림 7에서 보는 것과 같이 Matched Filter는 수신된 신호를 Register에 저장하고 매 회마다 Shift하면서 Local PN-code와 상관도를 비교한다. 이렇게 되면 1 PN chip마다 상관도ener지를 구할 수 있게 되므로 하나의 위상을 탐색하는데 걸리는 시간을 상당히 감소시킬 수가 있다.

PN chip과 Match되어 더해진 값은 Power Detector에서 채널상태에 따라 program 될 수 있는 임계값과 비교하여 '0'이나 '1'로 결정된다. 즉, 임계값을 초과하면 '1'을, 임계값에 미치지 못하면 '0'을 판단한다. 구현된 시스템에서는 길이가 256인 PN-code를 사용하였으므로 모든 chip이 일치하였을 경

우 최대값은 256이 된다. 따라서 그 중간 값인 128을 고정된 임계값으로 사용하였다. 빠른 실시간성을 보장하기 위하여 Matched filter의 구조는 연산속도가 다른 구조에 비하여 매우 빠른 Systolic Array구조를 적용하였다^{4, 5)}.

역 확산된 데이터는 Reed-Solomon Decoder에 의하여 오류가 정정되고 DES processor에 의하여 인증과정을 거치게 된다. 인증과정까지 모두 마친 메시지는 Local command와 비교하여 해당하는 명령을 수행하게 된다. 그림 8에 DS-SS방식 AFTS의 블록 다이어그램을 나타내었다.

IV. 시뮬레이션 결과

설계를 위한 합성틀은 ALTERA社의 Quartus II 4.0을 사용하였다. 그리고 시뮬레이션을 위하여 Mentor Graphics社의 시뮬레이션 툴인 ModelSim 5.7d를 사용하였다. 하드웨어는 송신기와 수신기 모두 ALTERA社의 FPGA를 사용하였다. 송신기는 Excalibur 시리즈인 EPXA1F484C-3을 사용하였고 수신기는 FLEX계열의 EPF10K100ARC240-3을 이용하여 구현하였다.

Excalibur칩은 내부에 ARM 922T core가 내장되어 있어 Flexible한 프로그래밍이 가능하다. 이 core는 최대 200MHz로 동작이 가능하고 주변 peripheral간에는 AMBATM Bus⁶⁾로 데이터 전송이 가능하다. 구현에 사용된 EPXA1은 1.8V로 동작하고 4,160 Logic Elements(LE)를 가지고 있으며 내부에 53,248 bits RAM을 내장하고 있다. 수신기에 사용된 EPF10K100ARC240은 내부에 4,992 LE를 가지고 있고 24,576 bits RAM을 내장하고 있으며 최대 204MHz로 동작할 수 있다.

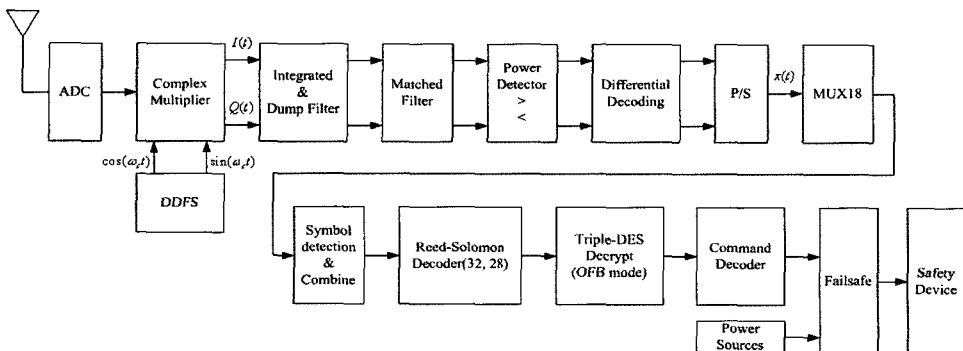


그림 8. DS-SS방식 AFTS의 블록 다이어그램

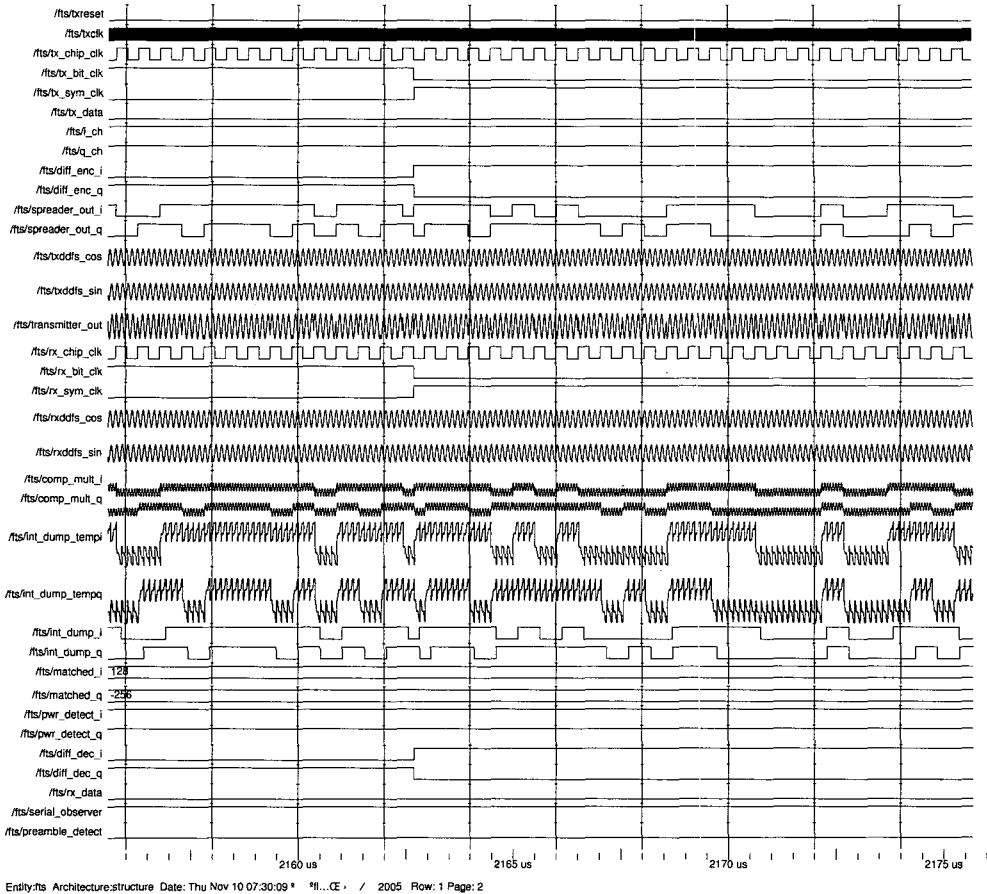


그림 9. DS-SS방식의 FTS MODEM의 전체 시뮬레이션 파형

합성되는 게이트의 크기는 각 회사들의 합성 톨의 성능에 따라 다를 수가 있으므로 본 논문에서는 하드웨어의 크기에 대해서는 중점적으로 다루지 않는다. 본 논문에서는 시스템의 구현이 목적이므로 구현된 시스템의 성능검증과 각 파형분석을 중점적으로 다룬다. 합성은 Speed Optimization하도록 합성하였고 시뮬레이션은 Timing 시뮬레이션을 보여준다. LCD Control을 위해서 ARM922T core를 이용하였고 Software Debugging은 ARM사의 ADS 1.2를 사용하여 Compile 및 Debugging을 하였다.

그림 9는 DS-SS방식의 FTS MODEM의 전체 시뮬레이션 파형이다. 구현된 MODEM은 19.6608MHz의 시스템 clock에서 4.8 kbps의 전송속도를 가지도록 설계되었지만 최대 40MHz까지 동작이 가능하기 때문에 9.6 kbps의 전송속도를 가질 수 있다. QPSK방식을 사용하였으므로 4.8 kbps일 때 초당 2,400 symbol이 전송되고 이는 614,400 cps의 전송률을 가진다.

확산코드의 길이를 정하기 위해서는 먼저 요구되는 성능을 알아야 하는데 본 논문에서는 요구되는 DS-SS FTS의 성능을 Bit Error Rate가 10^{-3} 정도인 시스템이라고 가정하였다. 이것은 최종적으로 요구되는 값이 아니고 prototype을 위한 값이며, 차후에 시스템분석과 비행중단시스템의 채널환경을 고려하여 채널의 Noise의 평균전력과 수신기의 평균전력을 구한 후 다시 계산 되어야 한다.

그림 10에서 DQPSK변조인 경우에 요구되는 BER이 10^{-3} 이면 E_b/N_0 는 약 10dB 정도 되어야 한다. E_b 는 P_R 과 T_b 의 곱으로 나타낼 수 있으므로 식 16과 같이 표현할 수 있다. 여기서 P_R 은 수신기에서 수신된 평균전력을 말한다.

$$\frac{E_b}{N_0} = \frac{P_R T_b}{N_0} \tag{16}$$

주파수대역 확산시스템의 processing gain L_c 는

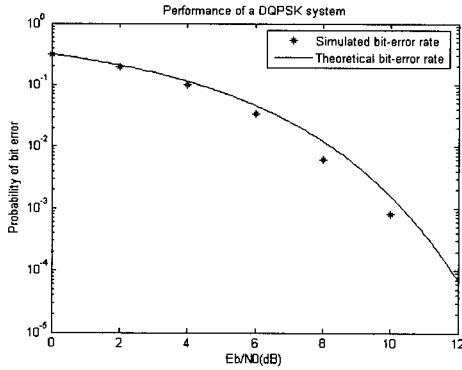


그림 10. DQPSK System의 BER성능

$$L_c = \frac{T_b}{T_c} \quad (17)$$

이므로 식 (16)은 식 (18)과 같이 표현된다. P_N 은 노이즈의 평균전력을 말한다.

$$\frac{E_b}{N_0} = \frac{P_R L_c T_c}{N_0} = \left(\frac{P_R}{W N_0} \right) L_c = \left(\frac{P_R}{P_N} \right) L_c \quad (18)$$

노이즈의 평균전력과 수신기에서 수신된 신호의 평균전력간의 비 P_R/P_N 을 4×10^2 이라고 할 때, L_c 는 250이 된다. 그러므로 PN-code의 길이는 250이 되어야 한다. 8-stage Gold code generator를 이용하여 PN-code를 생성할 경우 길이가 255인 PN-code가 생성된다. 그러나 길이가 255일 경우 시스템 설계적인 면에서 유연한 설계가 어렵다. 따라서 생성된 255길이의 Gold code에 1 bit를 padding시켜 길이가 256-chip인 코드를 사용하여 설계하였다.

Gold code를 생성하기 위하여 본 논문에서는 SSRG방식의 매커니즘을 이용하여 설계하였으며 설계한 Gold code의 Auto-correlation과 Cross-correlation 특성을 분석하였다. 그림 11은 1-bit padding하지 않은 255길이의 Gold code의 Auto-correlation function을 보여준다. 그림 12는 255길이의 m-sequence code에 1-bit를 padding하여 그것들의 Auto-correlation function을 구한 결과이다. 그래프를 보면 1-bit를 padding해도 성능저하가 많이 일어나지 않는다는 것을 알 수 있다. 위에서 사용한 4개의 m-sequence code를 2개씩 묶어 각각 I-ch PN-code와 Q-ch PN-code를 생성하였고, 그것들의 Auto-correlation function과 Cross-correlation function을 그림 13과 그림 14에 나타내었다. 그림 13에서, 상관값이 최대인 $\Delta Delay=0$ 일 때의 상관값은 $\Delta Delay \neq 0$ 인 구간에서의 최대값보다 약 8dB가 차이가 나

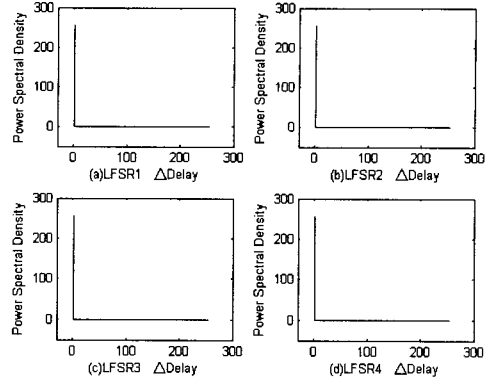


그림 11. 1-bit padding하지 않은 Gold code들의 auto-correlation function

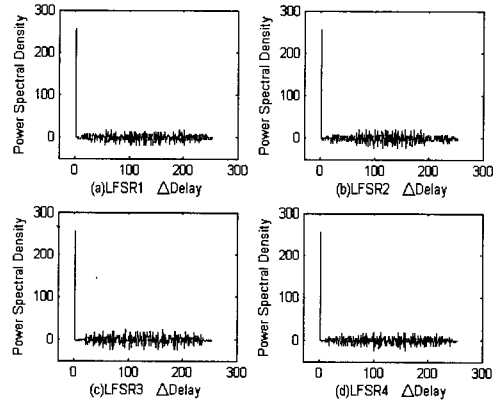


그림 12. 1-bit padding한 Gold code들의 auto-correlation function

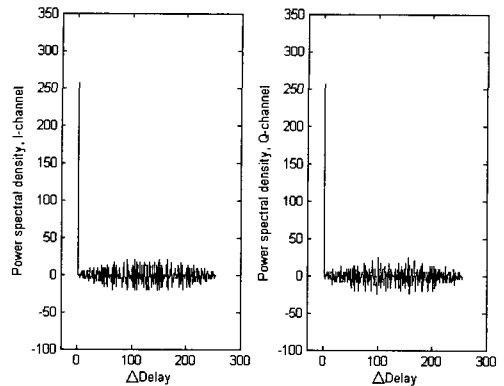


그림 13. I-ch과 Q-ch의 Auto-correlation function

기 때문에 성능 면에서 크게 나빠지진 않는다. 그리고 그림 14에서 Cross-correlation은 $\Delta Delay$ 가 약 30인 지점에서 상관도가 증가하는 peak가 발생하는데 이것 또한 최대 상관값보다 -7dB정도 낮다.

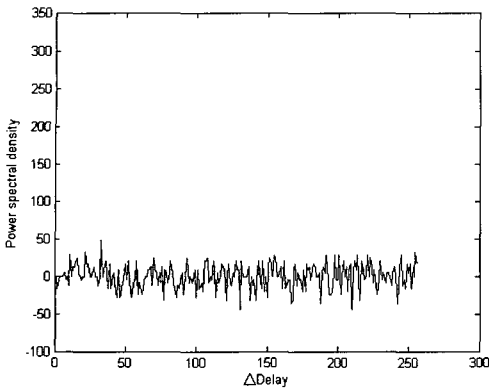


그림 14. I-ch과 Q-ch간의 Cross-correlation function

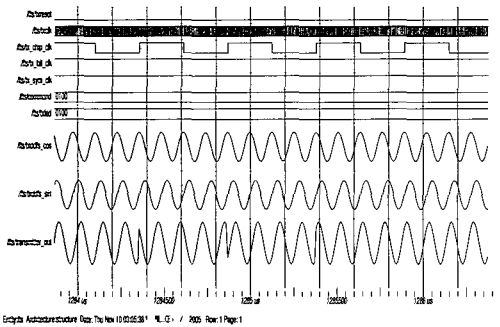


그림 15. DDFS의 출력파형

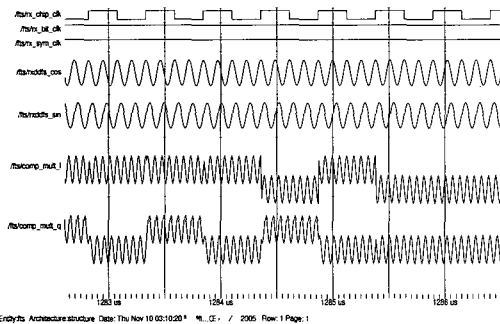


그림 16. 수신기의 DDFS출력파형과 Complex multiplier의 출력파형

그림 15에 나타난 그림은 DDFS에 사용된 sine과 cosine파형이다. 각각은 진폭이 5 bit, 위상이 4 bit의 분해능을 갖는다. 또, transmitter_out의 출력 신호는 위상이 0, $\pi/2$, $-\pi/2$, π 인 파형이 출력된다.

그림 16은 수신단의 DDFS에서 출력되는 sine과 cosine파형, 그리고 Complex multiplier의 출력파형을 보여준다. 그림에서 comp_mult_i와 comp_mult_q는 각각 I-ch과 Q-ch의 complex multiplier출력 신호이다.

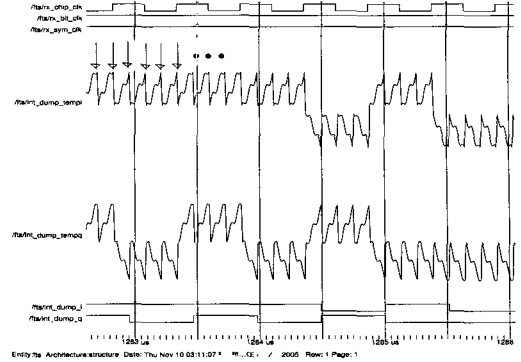


그림 17. Integrate and Dump filter의 출력파형

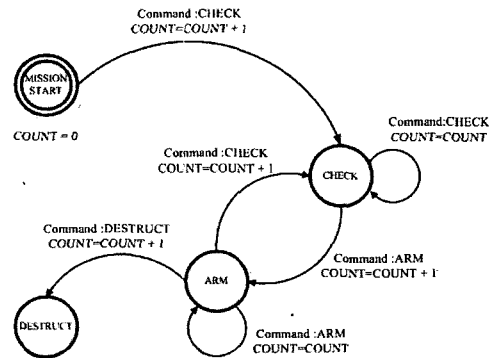


그림 18. Counter algorithm의 상태도

그림 17은 complex multiplier에서 carrier신호가 제거된 파형을 적분하고 적절한 타이밍에 샘플링하여 이진신호로 복원하는 Integrate and Dump Filter의 동작파형을 보여준다. 그림에서 화살표부분 지점에서 샘플링이 이루어지고 샘플링 된 데이터는 임계값과 비교하여 int_dump_i와 int_dump_q로 '1'이나 '0'의 데이터가 출력된다. 신호는 Differential Decoder와 RS(32, 28) Decoder, 그리고 DES Decoder에 의하여 Transmitter에서 전송되었던 원래의 데이터로 복호가 된다.

복호된 데이터는 Counter algorithm에 의하여 명령의 유효성을 검증한다. Counter algorithm이란 이전에 전송된 명령의 재사용을 방지하기 위한 알고리즘이다. Counter algorithm은 전송하는 명령이 변경될 때마다 전송 프레임의 count값을 1씩 증가시켜 수신기에서 이전에 수신했던 count값과 비교하여 크거나 같으면 명령을 수행하고, 그 값이 작으면 명령을 무시하게 된다. 이는 외부의 인증되지 않은 장치가 전파를 복사한 후 재전송하여 통신을 방해하는 행위를 방지하기 위함이다. 명령이 유효하다면 최종적으로 Command Decoder에 의하여 명령이

Actuator에게 전달된다. 그림 18은 Counter algorithm의 상태도를 보여준다.

V. 결론

본 논문에서는 주파수 대역확산방식의 비행중단 시스템을 제안하였고, 시스템에 사용되는 인증방식에 있어서 확산코드를 사용하여 기존의 비행중단시스템보다 정보의 기밀성과 보안성을 높였다.

하드웨어 구현은 RTL 수준에서 VHDL을 이용하여 구현되었고 ModelSim 프로그램에서 시뮬레이션하였다. 합성결과 GFTS는 최고 75.17 MHz로 동작하였고, AFTS는 최고 60.59 MHz로 동작하였다. 설계한 DS-SS FTS 모델은 4.8 kbps로 동작하도록 설계되었고, DES프로세서와 RS CODEC을 이용하여 보안과 오류정정성능을 높였다. 모델의 성능을 알아보기 위하여 송신기와 수신기간의 다른 확산코드를 사용하여 실험한 결과 FTS명령이 실행되지 않는 것을 확인 할 수 있었다.

설계한 DS-SS방식의 FTS는 coherent detection 방식이라 비행체 내부에서 발생하는 large shock와 vibration을 갖는 periodic신호들과의 phase noise에 민감하다. 따라서 이 부분은 아직 연구해야 할 과제로 남아있다.

참 고 문 헌

- [1] Range Safety Group(RCC), "SPECIAL REPORT RS-38," Nov. 1997.
- [2] Tuchman, Walter L., "Hellman Presents No Shortcut Solution to DES," *IEEE Spectrum*, Jun. 1997.
- [3] M. McLoone, J. V. McCanny, "High-performance FPGA implementation of DES schedule," *IEE Proc. -Circuits Devices Syst.* Vol.150, No.5, Oct. 2003.
- [4] J. Tierney, C. M. Radre, B. Gold, "A Digital Frequency Synthesizer," *IEEE Trans. on Audio and Electroacoustics*, Mar. 1971.
- [5] H. T. Kung, "Why systolic architectures?," *IEEE Computer 15(1)*, pp.37-46, 1982.
- [6] <http://www.arm.com>

임 금 상 (Keumsang Lim)

준회원



2004년 2월 세종대학교 정보통신공학과 학사

2004년 3월~현재 세종대학교 정보통신공학과 석사 과정
<관심분야> 통신신호처리, 채널 코딩, 암호학

김 재 환 (Jaehwan Kim)

준회원



2005년 2월 세종대학교 정보통신공학과 학사

2005년 3월~현재 세종대학교 정보통신공학과 석사 과정
<관심분야> Sensor network, WPAN

조 항 덕 (Hyangduck Cho)

정회원



1997년 방송통신대학교 전자계산과 학사

2000년 세종대학교 정보통신공학과 석사

2000년~현재 세종대학교 정보통신공학과 박사 과정
<관심분야> 통신신호처리

김 우 식 (Wooshik Kim)

정회원



1984년 서울대학교 전자공학과 학사

1986년 서울대학교 전자공학과 석사

1986년~1991년 미국 GIT 박사
1993년~1996년 한국통신 연구개발원 선임연구원

1996년~1999년 명지대학교 정보통신공학과 조교수
1999년~현재 세종대학교 정보통신공학과 부교수
<관심분야> 신호처리, 유무선통신, 의공학, sensor network