

전투기 무기체계의 Binary CDMA 무선네트워킹 기술에 관한 연구

김용성, 유호균, 편규범, 김동욱, 임용석

한국전자기술연구원

yskim@keti.re.kr, ghy1675@keti.re.kr, laotse@naver.com, dkim20200@keti.re.kr, busyatom@keti.re.kr

A Study on the binary cdma wireless networking technique of aircraft pod system

Yong Seong Kim, Ho Gyun Lyu, Gyu Beom Pyun, Dong Wook Kim, Yong Seok Lim

Korea Electronics Technology Institute

요 약

본 논문은 전투기 무기체계에서 사용되고 있는 무선 통신 네트워크 기술인 Binary CDMA 기술에 대하여 살펴보고 전투기 실내의 환경과 같은 무선 채널환경이 열악한 상황에서 QoS를 보장할 수 있는 최소 필요 SNR을 기준으로 송수신이 원활히 되는지를 예측해 보고, 기 구축되어 있는 Koinonia 칩셋을 적용한 무기체계와의 호환성을 위해 개조되어야 할 Guardian-S의 기능이 무엇인지 살펴본 후 Guardian-E ASIC 개발을 위해 수정해야 할 IP블록을 개조하여 FPGA 보드에 탑재 후 검증 결과를 제시한다.

1. 서론

본 논문에서는 무기체계의 통신망으로 운영 중인 Binary CDMA 기술에 대하여 알아보고, 기존 Binary CDMA 기술이 적용된 Koinonia 칩셋과 호환성을 위한 Guardian-E 칩셋 구현 방법을 알아본다.

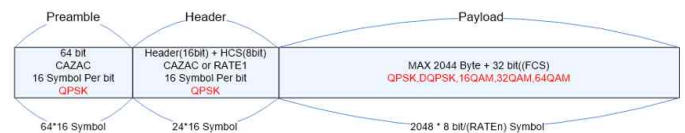
Binary CDMA 기술은 펄스폭을 조정하는 Pulse-Width CDMA (PW/CDMA), Phase를 조정하는 Multi-phase CDMA(MP/CDMA), 코드를 선택하는 Code Selection CDMA (CS/CDMA), CS/CDMA를 동시에 합쳐서 전송하는 CACB/CDMA 기술로 나눌 수 있고[1], Koinonia 칩셋에는 CACB/CDMA 기술이 탑재 되어 있다[2]. 특히 CACB/CDMA 기술은 입력비트를 이용하여 일시 코드를 선택한 후 산술 덧셈연산에 의해 더해서 전송하므로 기존 CDMA 확산기술의 속도가 일시 코드 사용 개수만큼 증가하게 된다. 한국 전자기술연구원(KETI)에서는 CACB/CDMA 기술을 이용하여 Koinonia 칩셋을 개발하였고 이 기술보다 복잡도를 간소화한 초소형 유사직교 부호화기를 개발하여 Guardian 시리즈 칩셋에 적용하였다. Guardian 칩셋중에서 현재 양산중인 Guardain-S 칩셋은 Koinonia 칩셋의 ISO표준 규격과 호환되며 초소형 유사직교 부호화기가 탑재되었고 암호화 엔진이 강화된 칩셋으로 무선 원격검침 시스템(HPGP, K-DCU), 국방 전투기 체계(KGGB), 공공 무선 영상전송 시스템(Wireless CCTV)등에 활용 중이다. 그러나 Guardain-S 칩셋은 Koinonia 칩셋에 적용된 옵션 사항인 비 표준규격의 기능을 적용하지 않아서, Koinonia 칩셋의 비 표준규격을 따르는 시스템과의 호환성이 해결되지 못하고 있다. 따라서 본 논문에서는 이러한 비표준 규격의 Koinonia 기능에 대해서 알아보고, 현재 제작 중인 Guardain-E 칩셋의 설계방안과 설계된 IP의 기능 검증 결과 그리고, 기존 무기체계와의 연동시험을 통한 기능검증 결과에 대해 알아보고자 한다.

II. 본론

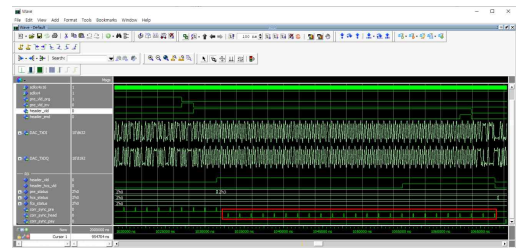
1. 물리계층의 PHY Header 확산방식 개조

먼저 Koinonia 칩셋에 옵션사항을 적용된 비표준 규격은 물리계층의 PHY Header 확산방식이다. 이 확산방식의 표준은 일시코드를 이용하는

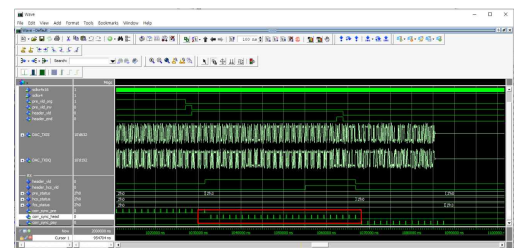
Binary CDMA의 RATE-1 확산방식이다. 그러나, Koinonia에서는 Binary CDMA RATE-1 확산방식과 CAZAC 확산방식을 소프트웨어에서 선택적으로 사용할 수 있도록 설계가 되어 있다. 전투기무기체계의 경우, 민간분야와 차별화를 위해 CAZAC 확산방식을 사용한다.



[그림 1] PHY packet 프레임 구성



[그림 2] Header mode : Walsh



[그림 3] Header mode: CAZAC

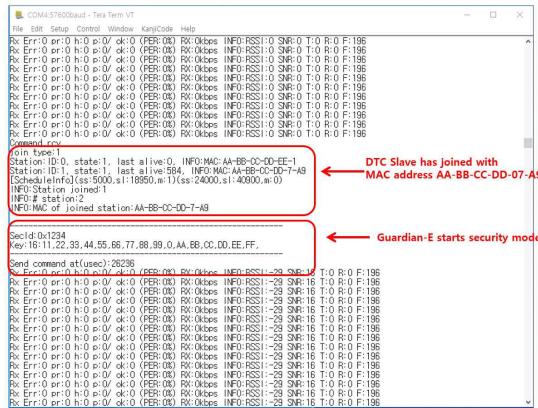
2. 암호화 프레임 형식 개조

두 번째로, MAC 프레임에 암호화 기능을 사용할 경우, Koinonia와 Guardian-S는 프레임 생성 방식이 아래 그림과 같이 상이하게 되어 있다. 따라서 Guardian-S 칩셋을 사용하는 전투기 무기체계에서는 암호화 방식 서로 상이하여 기존 Koinonia 칩셋을 적용하는 무기체계와 호환이 되질

않고 있는 실정이다. 따라서 Guardian-S 칩셋을 개조할 시, 두 가지 비표준규격에 대한 기능을 개조하여야 한다.



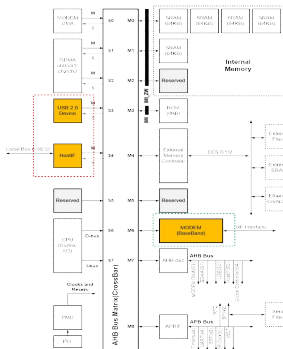
[그림 4] 암호화 프레임 형식비교-Koinonia(상), Guardian(하)



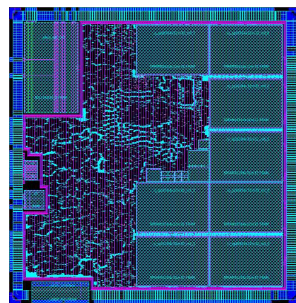
[그림 5] Guardian-E 와 DTC 간 암호화 패킷 송수신 과정

3. USB IP 개조

향후 무기체계 적용시 호스트와의 인터페이스를 간소화하고, 다양한 시스템에 쉽게 사용할수 있도록 USB인터페이스를 제공하였다. Guardian-S에서 제공하는 USB IP의 기능 검증을 통해 수정 및 개선사항을 적용하여 Guardian-E 제작에 적용하였다.



[그림 6] Guardian-E 내부구성도 [그림 7] Guardian-E ASIC P&R



4. KCMVP 검증필 제공을 위한 암호화 IP 개조

Guardian-E의 개발과정에서 암호화 패킷에 대한 기능검증을 위해 암호화 MAC 프레임 형성과는 별개로, 128/256 블록암호를 지원하는 암호화 엔진과 암호화 운영모드를 지원하기 위해, 암호화 엔진(ARIA, AES)과 다양한 운영모드(ECB, CBC, CTR, CCM, GCM)를 설계한 후 국정원 테스트 벡터 [4]입출력 시험을 수행 한 결과 국정원 테스트 벡터 모든 경우의 수를 만족시켰다. 이는 향후에 KCMVP 검증필 신청을 위한 기본 사항으로 설계가 되었다.

5. Guardian-E IP의 FPGA 보드레벨 검증

Guardian-E IP를 설계한 후, FPGA 보드 시험을 통해 기존 Koinonia를 사용하는 KGGB 장비의 DTC보드와 연동시험을 아래와 같이 수행하였고 시험 결과 암호화하는 패킷의 경우 송수신가능함을 확인하였다. Guardian-E의 모뎀블럭의 성능은 기존 Koinonia와 Guardian-S의 모뎀성능과 동일하게

-80dBm에서 SNR 10dB 이상을 확인하였고, 변조 방식별로

DQPSK변조시 17dBm@PER 1%(Packet 길이: 1023byte), Binary CDMA RATE-4 변조시 14dBm@PER 1%(Packet 길이: 512byte), Binary CDMA RATE-3 변조시 11dBm@PER 1%(Packet 길이: 200byte), Binary CDMA RATE-2 변조시 8dBm@PER 1%(Packet 길이: 100byte), Binary CDMA RATE-1 변조시 5dBm@PER 1%(Packet 길이: 50byte), 와 같이 확인되었다.



[그림 8] Guardian-E IP를 탑재한 FPGA 개발환경

Guardian-E IP를 설계하고, FPGA 보드상에 다양한 기능검증을 수행한 후, SMIC 0.13um 공정을 통해 Fab-in이 진행되었다. Die 사이즈는 6000 um X 6100 um, 패키지는 284 FBGA, 칩사이즈는 15mm x 15mm이다. Guardian-E ASIC칩의 시험은 향후 추진 예정이며, 칩 성능결과는 FPGA 보드 레벨 연동시험과 동일 할것으로 예상된다.

III. 결론

본 논문에서는 기존 전투기 무기체계에서 적용 중인 Koinonia 기반의 KGGB 무기체계와 통신이 호환되는 Guardian 기술에 대하여 살펴보고 Guardian-E 개발 시 개조해야 할 사항과 개조 결과물의 검증 결과를 제시 하였다. 또한 수정된 IP를 FPGA 보드 레벨에서 검증해보고, 이를 기존 KGGB DTC 보드와 연동 시험을 통해 모뎀 IP의 검증을 수행하였다. FPGA 보드 레벨의 모뎀 IP 성능은 기존 Guardian-S의 성능과 유사하였고 연동 시험을 통해 Koinonia와의 암호화 프레임이 원활하게 전송됨을 확인하였다. 검증된 Guardian-E IP는 ASIC 제작이 완료되어 2012년 6월경 시험 절차에 들어가고 향후 ASIC 칩셋에 대한 성능분석을 수행할 예정이다.

ACKNOWLEDGMENT

본 논문은 방위사업청의 무기체계 개조개발 사업의 “GPS 유도키트 수출을 위한 비행제어장치 및 인터페이스장치 개조개발” 과제의 지원을 받아 수행하였습니다.

참 고 문 헌

- [1] 안호성, 류승문, 나성웅, “Binary CDMA 소개”, JCCI, VI-A.1.1-4, April 2002
- [2] KETI, KOINONIA 표준규격서, 물리 계층과 데이터 링크 계층 규격 버전 ISO/IEC standard 24771, 2009
- [3] 국정원, “민관겸용 블록 암호 알고리즘 및 ARIA테스트벡터”, 2004.5
- [4] KISA, “<https://seed.kisa.or.kr/kisa/kcmvp/EgovVerification.do>”, 검증 대상 암호알고리즘 V3.0 테스트벡터