技術論文 J. of The Korean Society for Aeronautical and Space Sciences 42(7), 594-600(2014)
DOI:http://dx.doi.org/10.5139/JKSAS.2014.42.7.594

군통신위성 디지털 중계기의 간섭 회피 처리 구조 설계 및 구현

설영욱*, 유재선*, 정건진**, 이대일***, 임철민***

Design and Implementation of Interference-Immune Architecture for Digital Transponder of Military Satellite

Young-Wook Sirl*, Jae-Sun Yoo*, Gun-Jin Jeong**, Dae-Il Lee*** and Cheol-Min Lim***
Satrec Initiative Inc.*, Samsung Thales Co., Ltd.**, Agency for Defense Development***

ABSTRACT

In modern warfare, securing communication channel by combatting opponents' electromagnetic attack is a crucial factor to win the war. Military satellite digital transponder is a communication payload of the next generation military satellite that maintains warfare networks operational in the presence of interfering signals by securely relaying signals between ground terminals. The transponder in this paper is classified as a partial processing transponder which performs cost effective secure relaying in satellite communication links. The control functions of transmission security achieve immunity to hostile interferences which may cause malicious effects on the link. In this paper, we present an efficient architecture for implementing the control mechanism. Two major ideas of pipelined processing in per-group control and software processing of blocked band information dramatically reduce the complexity of the hardware. A control code sequence showing its randomness with uniform distribution is exemplified and qualification test results are briefly presented.

초 록

현대전에서는 적의 전자기파 공격에 대응하여 안전한 통신 채널을 확보하는 것이 매우 중요하다. 군통신위성 중계기는 차세대 군통신위성에 탑재를 위한 통신 탑재체로써 간섭 환경 하에서 지상 터미널 간의 신호를 안전하게 중계하여 전시 통신망을 유지하도록 한다. 본 논문에서 소개하는 위성중계기는 온보드 상에서 부분적인 신호처리를 수행하는데 위성 통신 링크를 저비용으로 제어할 수 있다. 이의 핵심 기능으로써 전송 보안 제어 기능은 통신 링크를 위협하는 간섭 신호에 대한 면역성을 확보한다. 보다 구체적으로 본 논문에서는 전송 보안 제어 기능을 구현하기 위한 효율적인 설계 구조를 소개한다. 핵심 아이디어로써 시분할 형태의 채널 그룹별 제어 코드 생성 및 금지 대역 정보에 대한 소프트웨어 처리 방법으로 전체 하드웨어 복잡도를 현저하게 낮출 수 있음을 설명한다. 생성된 결과 코드가 균등 분포의 임의성을 가짐을 예시하였으며, 우주 인증 시험 결과를 간략히 소개한다.

Key Words : Satellite Communication(위성 통신), Satellite Transponder(위성 중계기), Transmission Security(전송 보안)

† Received: April 1, 2014 Accepted: May 31, 2014
* Corresponding author, E-mail : yos@satreci.com
http://journal.ksas.or.kr/
pISSN 1225-1348 / eISSN 2287-6871

Ⅰ. 서 론

최근 개인용 무선 통신 기술이 급격히 발전하여 보급됨에 따라 현대인에게 무선통신 기기는 불가결한 생활필수품이 되었다고 볼 수 있다. 그러나 무선 통신 기술 발전과 더불어 그에 상응하는 통신 및 정보 보호의 필요성이 증대되고 있고, 특히 군용 통신에서는 통신 보안의 유지 여부가 유사시 국가와 민족의 존망을 바꿀 수도 있을 정도의 중요성을 갖는다고 할 수 있다. 통신 및 정보 보호를 위한 여러 가지 기술 분야가 있으며, 무선 통신 분야에서는 통신 신호 전달 매체에 대한 접근이 비교적 용이하므로 다양한 형태의 통신 신호에 대한 공격과 방어 기술이 있을 수 있다. 특히, 현대의 전자전에 있어서 전자보호(Electronic Protection: EP)기술은 아군의 전투 능력을 떨어뜨리거나 파괴하는 아군 또는 적군의 전자기 스펙트럼 영향으로부터 인력, 시설 및 장치를 보호하는 모든 활동을 포함한다.

전자보호 기술 중 효과적으로 사용하는 주요 기술로써 주파수 도약 (Frequency Hopping: FH) 방식이 있다. 이는 특정 광역 주파수 대역 내에서 유효한 협대역 통신 신호의 주파수를 빠른 속도로 끊임없이 변경함으로써, 적의 신호 탐지, 감청 및 간섭 신호를 무력화하고 안전한 통신 채널을 확보하는 기술이다[1]. 통신위성의 중계기를 통한 지상 단말 간의 통신은 상향과 하향 링크로 명명되는 두개의 단일 통신 링크를 통해 수행되는데 두 통신 링크 모두 간섭 신호에 노출될 수 있는 구조이므로 각각의 링크에 대한 통신 보안을 모두 유지할 수 있어야 한다.

본 논문에서는 차세대 군통신위성에 탑재될 위성중계기 설계 및 중계기에서 간섭 회피를 위한 코드화된 주파수 제어 패턴을 생성하는 통신 보안 알고리즘의 효율적인 구현 구조에 대하여 설명한다.

Ⅱ. 본 론

2.1 위성 중계기의 분류

위성 통신 시스템에서 위성 중계기 방식을 몇 가지 형태로 분류할 수 있는데, 굽은 파이프(bent-pipe transponder: BPT) 방식, 부분 처리(partial processing) 방식, 심볼 재생성 처리(symbol regenerative processing: SRP) 방식 및 패킷 스위칭 처리(full processing packet-switched) 방식이 있다[2].

먼저 BPT 방식은 전체 대역폭 내의 신호를 수신하여 재전송하는 방식으로, 대역 내에 간섭 신호가 존재할 경우 간섭 신호까지 증폭하여 보내기 때문에 간섭 신호에 의한 신호대 잡음비(signal-to-noise ratio: SNR) 손실이 유발되며 최종 단말 간 통신 성능을 저하 시킬 수 있다.

두 번째는 부분 처리 방식으로써 전체 대역폭보다 훨씬 작은 대역폭의 유효 신호를 상향 링크에 대한 협대역 주파수에 의해 정의되는 대역 필터를 통해 복원한 후, 하향 링크를 통해 상향 링크와는 다른 주파수 위치에 증폭하여 재전송한다. 이로써 대부분의 경우에 상향 링크에 인가되는 간섭 신호 제거할 수 있다. 본 논문에서 설명하는 위성중계기는 부분 처리 방식의 중계기로 볼 수 있다.

세 번째로 위성 수신부에서 채널별 필터링 뿐만이 아니라 수신 신호를 복조하여 원래의 상향 데이터 심볼을 복원한 후, 다시 변조 및 채널을 변화시켜 하향 링크를 통해 전송하는 방식으로써 SRP 방식이 있다. 그러나, 이 방식은 앞선 두 가지 방식에 비해 위성에서 처리해야 하는 복잡도가 급격히 증가하고, 운용상의 유연성도 부분 처리 방식에 비해 좋지 않다.

마지막으로 패킷 스위칭 처리 방식은 상향 링크에 대한 채널화, 복조, 복호화를 수행하고 하향 링크로 새로운 부호화, 변조, 채널 스위칭을 포함하는 방식으로써 보안성 측면에서는 가장 좋은 성능을 보이며 유연한 스위칭 기능을 가지나 복잡도가 가장 높다는 단점이 존재한다.

2.2 부분 처리 방식 중계기

2.2.1 시스템 형상

앞서 설명한 바와 같이 본 논문에서 설계 제작한 중계기는 부분 처리 방식의 위성중계기로써, Fig. 1과 같은 기능 구조를 갖는다. 즉, 상향 링크를 통해 수신된 협대역 신호는 임의의 해상도를 갖는 입력 필터를 통해 분리되고, 상향/하

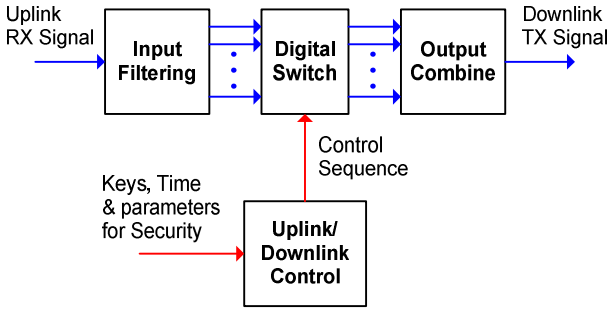

Fig. 1. Functional Diagram of the Transponder

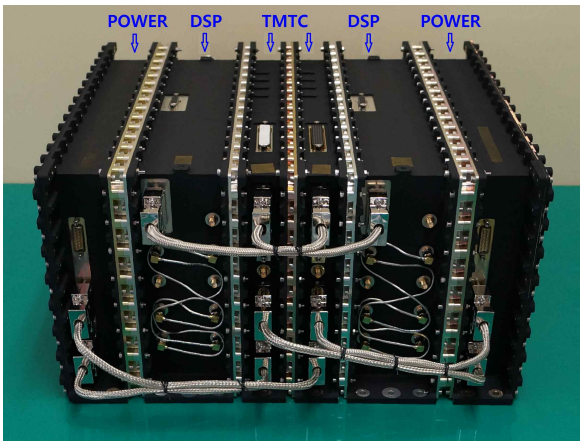

Fig. 2. Picture of the Transponder

향 링크 제어부(Uplink/Downlink Control)로부터 들어오는 코드에 의해 특정 시간 동안 입력 필터의 출력이 선택된다. 그 후, 선택된 출력은 상향과는 다른 순서 코드에 따라 스위칭되며 각 채널별로 설정된 이득 값에 따라 증폭된 후 출력부에서 결합되어 하향 링크로 전송된다. 한편, 상향/하향 링크 제어 블록은 제어 순서 코드를 생성하는 기능을 하며, 이를 위한 입력 변수로써, 통신 보안 키 값과 시간 정보 및 기타 정보를 바탕으로 상향/하향 링크 제어 기능을 수행한다.

본 논문에서 설명하는 설계 및 구현 구조의 핵심은 바로 이 상향/하향 링크 제어 블록에서 전송 보안 알고리즘을 처리하는 것에 대한 것이다. 실제 설계 제작한 위성중계기 장치의 하드웨어는 전원부(POWER), 제어부(TMTC), 신호처리부(DSP)의 세 부분으로 나눌 수 있으며 각각은 이중화 구조로 설계 제작 되었으며, 실제 형상을 Fig. 2에서 볼 수 있다.

기존의 유사한 위성중계기로써는 무궁화5호 위성에 탑재된 중계기가 있으나, 성능 및 채널 용량 면에서 본 논문에서 소개하는 중계기와는 큰 차이가 있다[4]. 즉, 기존 위성 중계기는 단 두 개의 채널만을 지원하므로 각각 채널에 대한 제어부를 독립적으로 두고 아날로그 방식의 주파수 합성기를 채용하여 구현하였으나, 본 논문에서 소개하는 방식의 위성 중계기는 수십 개의 채널을 가지므로 기존 방식을 사용할 경우 엄청난 크기의 하드웨어를 필요로 한다. 따라서 본 논문에서는 다수의 채널 그룹을 효율적으로 지원하기 위하여 통합적인 제어부와 디지털 신호 처리 기술을 통해 새로운 구조의 중계기 설계 방식과 관련된 다수의 채널 그룹에 대한 통합적인 제어 순서 코드 생성 구조의 설계 및 구현에 대한 내용을 주로 다룬다.

2.2.2 제어 순서 코드 생성 설계 구조

전송 보안 기능은 통신 보안 기능과 함께 보안을 위한 핵심 기능으로써 전송 매체 상에서 보호 기능을 담당하고 통신 보안은 암호화(encryption)를 통한 메시지 수준의 보호 기능을 담당한다. 일반적인 전송 보안 기능을 위해 정의되는 입력 변수는 암호 키, 정확한 시간, 운용자의 채널 선택 값 및 허용된 주파수 영역이 있으며, 출력 값으로는 동기 패턴, break-in 패턴, 망 진입 변수 및 제어 순서 코드가 있으나[1], 본 논문에서는 제어 순서 코드 생성 부분에 대해 초점을 두고 있다. 제어 순서 코드를 제외한 나머지 출력 변수 값들은 본 논문의 범위에서 제외된다. Fig. 3에서 보는 바와 같이 제어 순서 코드 생성 블록은 크게 명령 제어부, 시간 제어 부, 암호키 제어부, 암호화 처리부 및 전송 보안 코드 처리부로 구성된다. 명령 제어부는 위성 버스를 통해 지상에서 전달 받은 망 제어 명령에 따라 위성중계기의 모든 요소를 제어할 수 있다. 시간 제어부(Time Control)는 제어 주기에 맞추어 기준 시간을 발생하는 카운터인데, 카운터의 초기화, 일시 정지 및 재시작, 새로운 값 설정 등에 관련된 제어 기능을 수행하며 생성된 시간 값은 암호화 처리부의 입력으로 사용된다. 암호키 제어부(KEY control)는 키의 저장, 변경, 적용 등 키 관리와 관련된 모든 기능을 수행하며, 암호화 처리부(Encryption Engine)는 시간 값과 암호키 값을

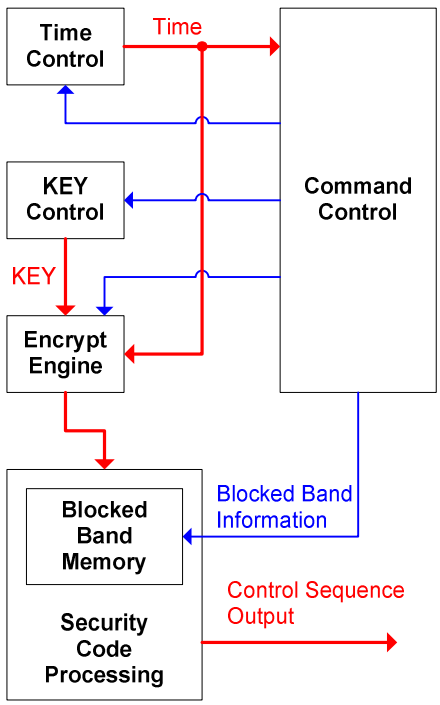

Fig. 3. Control Code Generation

입력 받아 특정 암호화 알고리즘을 통해 제어 코드 생성의 기반이 되는 일정 길이의 랜덤 데이터를 매 제어 시간 마다 출력한다. 마지막으로 전송보안 코드 처리부(Security Code Processing)는 생성된 랜덤 데이터를 이용하여 운용자가 미리 설정한 금지 대역 정보를 피하여 각 사용자 그룹별 상향/하향 링크에 채널을 할당하는 제어 순서 코드를 최종적으로 생성한다.

이와 같은 제어 순서 코드의 생성은 최대 N 사용자 그룹에 대하여 수행되어야 하는데, N개의 코드 생성 블록을 사용할 경우, 복잡도가 N배로 증가하여 위성 하드웨어 설계 상 상당한 부담이 되므로 하나의 하드웨어 자원을 사용하여 모든 사용자 그룹을 처리하는 시분할 방식으로 설계 되어야 한다.

2.2.3 전송 보안 코드 처리

전체 통신 대역폭을 공유하는 사용자 그룹이 최대 N개일 경우, 각 그룹별 상향/하향 제어 순서 코드는 서로 배타적으로 설계되어야 한다. Fig. 3의 전송 보안 코드 처리부는 암호화 엔진으로부터 매 제어 주기 마다 변하는 첫 번째 그룹 위치 정보와 그룹 간 이격 정보 및 랜덤 코드를 수신하여 N개의 그룹에 대한 제어 순서 코드를 생성한다. Fig. 4에 상세한 제어 순서 코드 처리 블록도를 도시하였다. 그림에서, 사용되는 기호의 의미는 다음과 같다. N은 사용자 그룹 개수이며, L = $\lceil \log_2(N) \rceil$ 로 표기할 수 있는데 $\log_2(N)$ 보다 큰 정수 중 가장 작은 수를 의미한다. P는 채널 주파수 위치를 표시하는 해상도와 관련된 값으로써, 전체 그룹 주파수 위치를 P 비트로 표기하므로 그룹 주파수는 산술적으로는 2^P

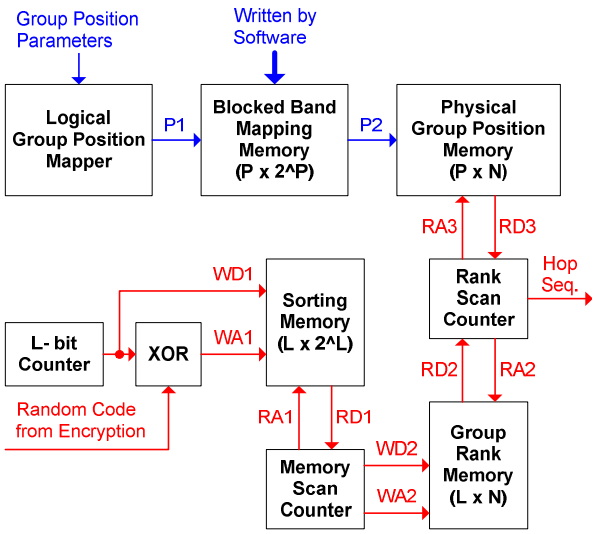

Fig. 4. Code Processing Details

개의 서로 다른 위치를 가질 수 있다.

그림에서 아래 쪽 부분의 L-비트 카운터로 시작하여 그룹 순위 메모리(Group Rank Memory)에 이르는 경로에서는 각 그룹의 상대적인 위치를 결정하기 위한 처리를 수행한다. 위쪽 부분에서는 각 그룹별 주파수 위치를 일련의 계산 과정을 통해 물리적 그룹 위치 메모리 (Physical Group Position Memory)에 기록한다. 그 후, 앞서 계산된 그룹 순서 메모리의 데이터(RD2)와 물리적 그룹 위치 메모리의 데이터(RD3)를 동시에 순차적으로 읽어 내면서 그룹 순서 값 즉, 0~(N-1)값에 따른 그룹의 해당 그룹의 P 값 즉, 물리적 위치 값을 결정하여 제어 순서 코드로 전송하게 된다. 여기서 물리적 그룹 위치 메모리의 내용을 결정하기 위한 입력 변수들은 암호화 엔진으로부터 수신한 암호화된 정보 및 운용자에 의해 설정되는 금지 대역(Blocked Band)정보가 있다. 금지 대역 정보 처리에 관한 내용은 다음 절에서 설명하도록 한다.

이와 같은 제어 순서 코드 처리 과정의 처리 속도를 클럭 기준으로 살펴보면 첫 번째 정렬 메모리에 쓰기 주기 동안 2^L 사이클, 정렬 메모리를 스캔하여 그룹 순위 메모리에 쓰는 2^L 사이클과 최종적으로 물리적 그룹 위치 메모리 및 그룹 순위 메모리의 값을 읽어 내어 제어 코드를 전송하는 L 사이클 만큼의 시간이 소요된다. 또한, 정렬 메모리는 현재의 제어 주기와 다음 제어 주기에서 갱신되지 않는 위치가 일치하지 않으므로 매 제어 주기 마다 초기화 되어야 하며, 기화 하는데, 2^L 사이클 만큼의 시간이 소요된다.

물리적 그룹 위치 메모리를 쓰는 경로는 그룹 순위 메모리를 쓰는 경로와 독립적이며, 단지 L 사이클 만큼의 클럭 주기만 소요되므로 속도 측면에서는 관심 경로에서 제외 된다. 따라서 단일 제어 주기 동안의 제어 순서 코드 처리 소요 시간은 처리 클럭 주기를 T_s, 암호화 처리 시간을 T_e, 제어 주기를 T_{cycle} 이라고 할 때, 수식 (1)과 같은 조건이 성립되도록 T_s와 T_e를 설정하여야 한다. 일반적으로 T_s는 T_{cycle}에 비하여 충분히 작은 값이 되고, T_e는 수십 사이클의 T_s로 구현이 가능하므로 매 제어 주기 마다 모든 그룹에 대한 제어 코드 생성이 가능하다.

$$T_s \times 3 \times 2^L + T_e < T_{cycle} \quad (1)$$

2.2.4 금지 대역 정보 처리

일반적인 전송 보안 운용 개념 상, 금지 대역 정보는 매 제어 주기 마다 변경되는 것이 아니며, 전자전지원 (Electronic Warfare Support: ES)

기술에 의해 탐지된 간섭 신호 특성에 따라 위성중계기 운용 시작 이전에 설정된다. 또한, 금지 대역 정보는 상당히 복잡하고 다양한 형태로 설정이 가능해야 하므로 하드웨어 보다는 소프트웨어로 처리하는 것이 바람직하다. 즉, 다수의 금지 대역이 존재할 경우, 그에 상응하는 비교 논리 회로가 필요하며 이를 하드웨어로 구현하는 것은 상당한 복잡도 증가를 유발한다. 따라서, Fig. 4에서 위쪽 두 개의 블록인 논리적 그룹 위치 설정부 (Logical Group Position Mapper)와 금지 대역 설정 메모리(Blocked Band Mapping Memory)를 통해 유연한 금지 대역 정보 처리가 가능하다. 즉, 논리적 그룹 위치 설정부는 매 제어 주기마다 일련의 정보 처리를 통해 전체 채널 그룹의 위치(P1)를 1차적으로 결정하고, 운용자가 설정한 금지 대역 정보에 따라 통신 대역폭 내 모든 주파수 위치에 대한 일대일 대응 관계를 소프트웨어를 통하여 미리 금지 대역 설정 메모리에 저장해 두면, 하드웨어는 단순히 표참조 방식(Look-Up-Table)으로 실제 물리적 그룹 위치(P2)를 실시간으로 결정할 수 있다. 또한, 금지 대역 설정 메모리는 운용 중 끊임없는 정보 갱신을 위하여 이중 메모리 형태로 구현하여, 새로운 금지 대역 정보를 갱신 하는 동안에도 이전의 정보를 사용할 수 있도록 하였다.

일정 시간 동안 유지되는 간섭 신호는 금지 대역 정보 설정을 통해 회피 및 제거가 가능하나, 제어 주기 수준의 짧은 운용 그룹 대역폭 내의 간섭 신호에 대해서는 위성중계기의 신호처리부에서 실시간 탐지 및 제거가 가능하며, 제거된 간섭 신호와 함께 발생하는 사용자 신호의 손실은 위성중계기를 통하여 통신하는 단말과 단말 간의 오류 분산 및 정정 알고리즘을 통해 극복할 수 있다.

2.2.5 코드 생성 결과 예

앞서 설명한 바와 같이 본 논문은 암호화 알고리즘 자체를 제안하는 것은 아니며, 알려진 암호화 알고리즘을 이용하여 생성된 임의의 데이터를 바탕으로 다수의 그룹에 대한 제어 순서 코드를 생성하는 효율적인 기능 설계 및 구현 방법의 하나를 제시한다. 아울러, 제시된 구조를 통해 생성된 제어 순서 코드는 특정 주파수에 편중됨이 없이 균등한 분포를 갖는 의사잡음순열(Pseudo Noise Sequence: PNS) 형태이어야만, 통신 신호의 피탐 및 간섭을 최소화할 수 있다[1].

본 논문에서 설명하는 방법을 통해 생성한 제어 순서 코드의 주파수 위치를 Fig. 5에 히스토그램으로 예시하였다. 즉, 시간 값의 변화에 따라

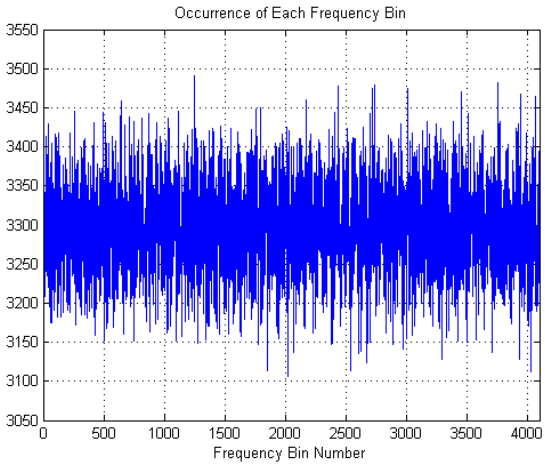

Fig. 5. Occurrence of Frequency Bins

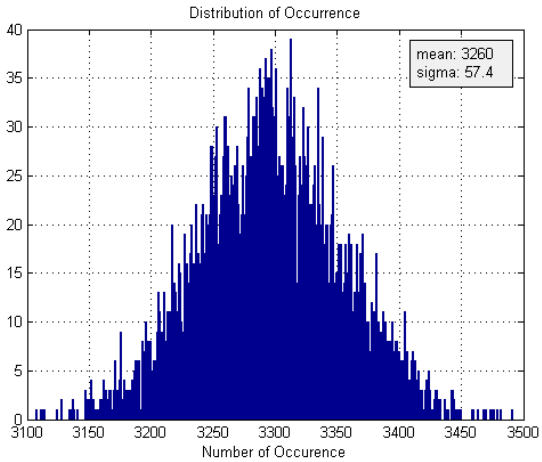

Fig. 6. Distribution of Occurrence

특정 그룹의 주파수 위치를 나타내는 코드는 그림에서 보는 바와 같이 특정 주파수에 편중됨이 없는 균등 분포를 갖는 랜덤 값으로 나타나며, 모든 다른 그룹 및 상향/하향 링크에 대해서도 유사한 형태의 균등 분포를 갖는다. 그림에서는 도시되는 샘플 수를 보다 많이 표시하기 위하여 모든 그룹에 대한 주파수 위치를 구별 없이 도시하였다. 또한, 각 그룹 주파수 위치의 발생 빈도는 Fig. 6과 같이 정규 분포의 특성을 나타내는데, 본 생성 예에 대해서 평균 발생 빈도 3260회를 중심으로 약 57회의 표준 편차를 보였다.

2.2.6 우주 인증시험

본 논문에서 소개한 위성중계기의 우주 인증을 위하여 우주환경 시험 및 발사환경 시험을 수행하였다. 우주환경 시험은 정지 궤도 위성이 겪는 고진공 상태에서 열적 변화에 대하여 위성중계기의 동작 성능을 측정하는 열진공 시험으로써, 비 동작 생존 (non-operating survival) 검증

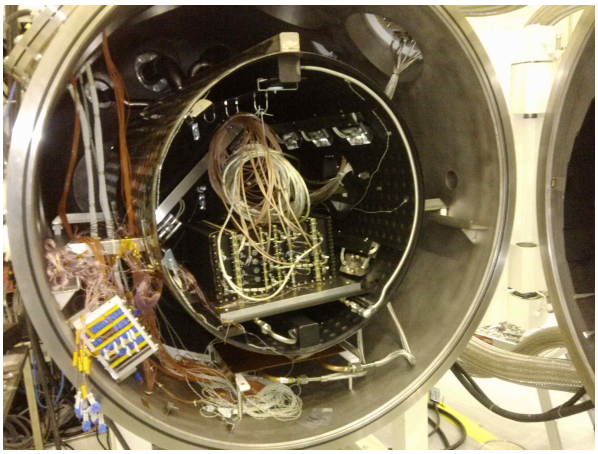

Fig. 7. Thermal Vacuum Test

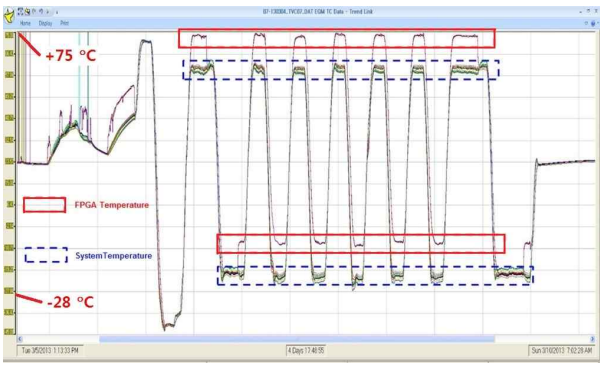

Fig. 8. Thermal Vacuum Test Result

Fig. 9. Vibration Test

을 위한 1 사이클과 7 사이클의 고온 저온 시험으로 구성된다. 고온 저온의 시험은 마지막 사이클을 제외하고 각각 2시간의 온도 유지 시간(dwell time) 이후, 성능 시험을 실시하였으며, 마지막 고온 저온 사이클은 4시간의 온도 유지 시간을 적용하였다. 위성중계기 내부의 관심 부분에 대하여 총 16개의 온도 센서를 적용한 후, 열진공 시험을 Fig. 7과 같이 실시하였으며, 위성중계기의 우주인증 모델에 대한 기계 및 전자부의 열적인 안정성과 열진공 환경에서의 시스템 기능 및 성능을 검증하였다[5-6]. 특히, 온도 기능 성능 시험의 인증 기준 온도인 -20 ~ +60 °C 구간에서 주 관심 대상 소자인 신호처리부 FPGA의 온도 변화는 저온 및 고온에서 각각 약 -10 °C와 +75 °C 로 나타났으며, 열진공 시험 이전에 실시한 열주기 시험에 비하여 충분한 열적 마진을 갖는 것을 확인하였다. Fig. 8에서 간략한 열진공 시험 결과의 그래프를 도시하였다. 그림에서 푸른색 점선 표시 부분이 위성중계기의 온도 기준점의 온도를 붉은색 실선 부분이 관심 전자소자인 FPGA의 온도를 나타내었으며, 동작 중 일정 온도 범위 내에서 유지됨을 확인하였다.

또한, 위성 발사 시 위성중계기가 겪게 되는 진동 및 충격 영향에 의한 위성중계기의 구조적 내성 검증을 위하여 정현파 진동(Sine Vibration), 랜덤 진동(Random Vibration) 및 충격(Shock) 시험을 Fig. 9와 같이 실시하였다. 각 시험 전후로 저준위검사(Low Level Survey: LLS)를 통하여 시험 전후간 모드 변화를 측정하였으며 모드 주파수 변화가 1 ~ 2.5%로 나타나 공차 범위인 5% 이내를 만족함을 확인하였고, 각 시험에 대하여 위성중계기의 설계 및 제작 상에 구조적인 문제가 없음을 확인하였다[5-6].

III. 결 론

본 논문에서는 군통신위성에 탑재될 위성중계기에서 간섭 회피를 위한 상향/하향 순서 코드를 생성하는 전송 보안 처리 기능의 효율적인 구현 구조를 제시하였다. 전체 통신 대역폭 내에 존재하는 여러 개의 채널 그룹에 대한 제어 코드를 각각의 그룹 별로 동일한 하드웨어의 병렬 구조가 아닌 단일 구조를 사용한 시분할 방식 및 유연한 설정을 제공해야 하는 금지 대역 정보 처리 부분을 소프트웨어와 분담하는 방식으로 하드웨어 복잡도를 최소화 하였다. 또한, 일반적인 병렬 구조 대비 시분할 단일 구조에서 대두되는 동작 속도의 증가 정도는 최근의 대부분 디지털 처리 소자의 동작 속도가 감당할 수 있는 수준이며, 그럼에도 불구하고 단일 구조의 단점으로써 고속 동작으로 인한 전력 소모의 증가를 꼽을 수 있으나, 병렬 구조의 복잡도 상승으로 인한 전력 소모 증가를 고려하면 충분히 단점을 극복하는 효율성을 확보할 수 있다. 본 논문에서 제시하는 간섭 회피 처리 구조에서 암호화 알고리즘 자체에 대한 것은 아니며, 일반적으로 알려진 암호화

방식을 채용하여 간섭 회피 처리 구조를 설계 구현하여 군통신위성 중계기를 제작하였으며 우주 환경시험 및 발사 환경시험을 통해 우주 인증을 완료하였다.

References

1) Roger J. Sutton, Secure Commmunications Applications and Management, *John Wiley & Sons*, 2002.

2) S. M. Sussman and P. Kotiveeriah, " Partial Processing Satellite Relays for Frequency-Hop Antijam Communications," *IEEE Trans. Commun.*, Vol. COM-30, no. 8, Aug. 1982, pp. 1929-1937.

3) Juan M. Rodriguez Bejarao, Ana Yun, and Borja De La Cuesta, "Security in IP Satellite Networks: COMSEC and TRANSEC integration aspects," *6th Advanced Satellite Multimedia Systems Conference (ASMS) and 12th Signal Processing for Space Communications Workshop (SPSC)*, Sept.. 2012.

4) R. Novello, L. Simone, F. De Tiberis, S. Paolucci, F. Barletta, D. Gelfusa, S. Cocchi, D. Fiore, R. Viola, I. Martinazzo, G.Lippolis, A. Bernardi, F. Autelitano, N. Salerno, M. Delfinom, P. Panella, F. Felici, V. Piloni, and M. C. Comparini, "The Koreasat 5 Secure Communication System: Design, Development & Performance,", *IEEE Aerospace Conference*, Mar. 2006.

5) ECSS-E-ST-10-03A, "Space Engineering, Testing," Feb. 2002.

6) ECSS-E-ST-10-03C, "Space Engineering, Testing," June 2012.