技術論文

통신위성 원격측정명령처리기 성능검증모델 원격명령 암호복호 검증

김중표*, 구철회*

Telecommand Decryption Verification for Engineering Qualification Model of Command Telemetry Unit in Communications Satellite

Joong-Pyo Kim* and Cheol-Hea Koo*

ABSTRACT

In this paper, the decryption function of CCSDS telecommand of CTU EQM for the security of communications satellite was verified. In order to intensify the security level of DES CFB decryption algorithm applied to CTU EM, 3DES CFB decryption algorithm using three keys is implemented in the CTU EQM. As the decryption keys increased due to the 3DES algorithm, the keys and IV are stored in PROM memory, and used for the telecommand decryption by taking the keys and IVs corresponding to the selected key and IV indexes from the memory. The operation of the 3DES CFB is validated through the timing simulation of 3DES CFB algorithm, and then the 3DES CFB core implemented on the A54SX32 FPGA. The test environment for the telecommand decryption verification of the CTU EQM was built up. Through sending and decrypting the encrypted command, monitoring the opcodes, and confirming LED on/off by executing the opcodes, the 3DES CFB telecommand decryption function of the CTU EQM is verified.

초 록

본 연구는 통신위성 원격측정명령처리기 성능검증모델 CCSDS 원격명령 암호복호 검증에 관한 것이다. 원격측정명령처리기 실험모델에 적용되었던 DES CFB 암호화 알고리즘의 보안성을 보다 강화하기 위해 3개의 키를 사용하는 3DES CFB 알고리즘을 원격측정명령처리기 성능검증모델에 구현하고 그것의 동작을 검증하였다. 3DES CFB 알고리즘에 따른 증가된 KEY와 IV를 위해 외부에 PROM을 두도록 하고 설정된 Index에 대한 키 및 IV를 가져와서 복호화 하도록 하였다. 설계된 3DES CFB 코어의 타이밍 시뮬레이션을 통해 동작 검증 후 Actel사의 A54SX32 FPGA에 구현하였다. 원격측정명령처리기 성능검증모델의 원격명령 암호 복호화 기능 검증을 위한 시험환경을 구축하고 원격측정명령처리기 성능검증모델에 원격명령 전송, 암호 복호화 후 수행코드 모니터링 및 수행에 의한 LED On/Off 확인을 통해 3DES CFB 원격명령 복호화 기능을 검증하였다.

Key Words : Decryption(복호화), Encryption(암호화), Telecommand(원격명령)

Ⅰ. 서 론

정지궤도 통신위성의 버스체 전장품들은 12~15년 이상의 정지궤도 우주환경에서도 높은 신뢰성 및 가용성을 갖는 설계 및 제작 기술을 필요로 하고 있다. 미국 및 유럽 등의 대형 위성 제

† 2004년 1월 10일 접수 ~ 2005년 6월 14일 심사완료
* 정회원, 한국항공우주연구원 통신해양기상위성사업단 체계종합그룹
연락저자, E-mail : jpkim@kari.re.kr
대전시 유성구 어은동 45

작업체들은 고유 위성 버스에 최적화된 전장품 설계, 제작 및 인증 기술을 확보하고 있으며, 수십년간의 축적된 첨단 기술들에 대한 기술 전수 규제를 국가 기술보호 및 경쟁력 강화를 위해 더욱 심화하고 있는 실정이다.

이런 상황에서 국내에서는 처음으로 정지궤도 통신위성 전장품 개발 기술 확보 및 향후 정지궤도 통신위성 버스체의 전장품으로의 활용을 위해 통신위성 원격측정명령계(TC&R, Telemetry, Command and Ranging)의 구성품들 중의 하나인 원격측정명령처리기(CTU, Command Telemetry Unit)를 선정하고 3개년에 걸쳐 개발하여 왔다. 1차년도에는 원격측정명령처리기 상세설계 후 CCSDS 원격명령 포맷에 DES CFB[1]를 적용한 원격명령 암호복호기 시제품 제작 및 시험을 통한 원격명령 암호화 복호 기능검증을 완료하였으며[2], 2차년도에는 원격측정명령처리기 실험모델(EM, Engineering Model) 제작 및 시험을 통해 DES CFB 원격명령 암호화 복호 후 명령 수행 및 텔레메트리 처리 기능을 포함한 전체 성능을 검증하였다[3].

3차년도에는 원격측정명령처리기 실험모델에서 사용하였던 원격명령 암호화 알고리즘인 DES의 보안 강화를 위해 3개의 키를 사용하는 3DES 암호화 알고리즘을 적용하여 원격명령 보안기능을 강화한 성능검증모델(EQM, Engineering Qualification Model)을 제작하고 기능 시험 및 우주환경 시험을 통해 모든 성능을 검증하였다.

본 논문에서는 원격명령 암호화 보안강화를 위해 실험모델에서 기 구현된 다중 키/다중 IV 활용[3] 및 명령 재공격(Replay Attack)[4]을 막기 위해 ACC(Authenticated Command Counter)를 사용한 것 외에 DES CFB 암호화 알고리즘 자체의 취약성을 보다 강화하기 위해 3개의 키를 사용하는 3DES CFB 알고리즘의 구현 및 검증에 대한 것이다. 3 개의 키를 사용하는 방법으로는 적정한 보안성 및 메모리 사용을 고려하여 KEY1=KEY3≠KEY2가 되도록 하였다. 3DES CFB 코어를 설계하고 타이밍 시뮬레이션을 통해 최적화한 뒤 설계된 3DES CFB 코어는 Actel사의 A54SX32 FPGA에 구현하였다. 3DES로 변경되면서 FPGA내의 게이트 수와 늘어난 키 값으로 인해 실험모델과 같이 FPGA 내부 버퍼 공간을 확보할 수가 없어 외부 PROM에 키 및 IV 값들을 저장하도록 하였고 설정된 키 인덱스 및 IV 인덱스에 해당하는 키 및 IV 값들을 가져와서 복호화 하도록 구현하였다. 성능검증모델의 성능을 검증하기 위하여 시험환경을 구축하고 암호화된 원격명령 전송, 암호 복호화 후에 원격명령 데이터의 모니터링, 수행코드 실행에 의한 LED On/Off 확인, 1553B 통신을 통해 OBC에 전달된 Bus 명령의 전달 확인을 통해 3DES CFB 원격명령 복호화 기능을 모두 검증하였다.

II. 본 론

2.1 성능검증모델 구성 및 주요 기능

원격측정명령처리기는 TC&R의 원격측정명령처리를 담당하는 베이스밴드(Baseband) 전장품으로 수신 안테나를 거쳐 명령수신기(CMR, Command Receiver)에 의해 복조되어 전달된 CCSDS 원격명령 포맷의 유효성 확인, 원격명령 암호 복호 및 명령 검증을 한 뒤 위성체구성명령(SCC, Spacecraft Configuration Command)의 경우는 위성체 구성의 상태를 직접 제어하고 버스 명령(Bus Command)의 경우는 MIL-STD-1553B 워드로 포맷된 후 MIL-STD-1553B 버스를 통해 OBC(Onboard Computer)로 전달한다. 또한 OBC에 의해 수집된 SOH(State of Health) 데이터를 MIL-STD-1553B 버스를 통해 받은 후 CCSDS 텔레메트리 패킷 프레임으로 포맷한 뒤 지상국에 송신 안테나를 통해 전송하기 위해 RF 비콘송신기(BTX, Beacon Transmitter)에 전달하는 기능을 한다. Fig. 1에 TC&R 서브시스템의 블록 다이어그램을 나타내었다.

이러한 기능들을 수행하기 위해 원격측정명령처리기 하드웨어는 다음과 같은 보드들로 구성된다.

a) Uplink/1553B 보드
b) Telemetry 보드
c) Command 보드
d) EPC 보드
e) Backplane 보드

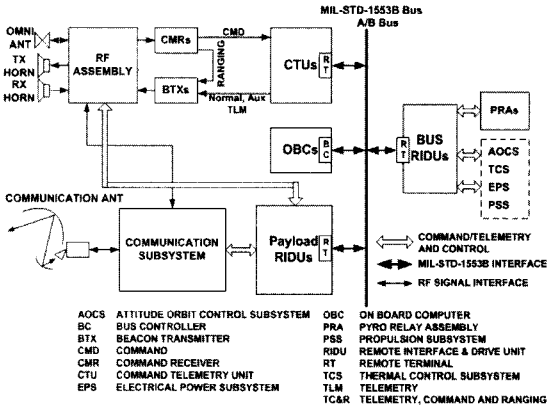

Fig. 1. Block Diagram of TC&R Subsystem

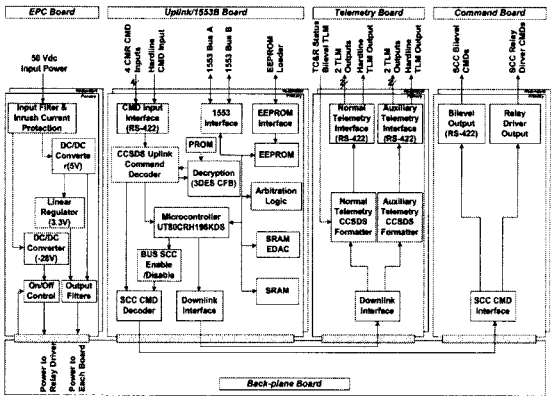

Fig. 2. Configuration of CTU EQM

원격측정명령처리기의 보드 구성도를 Fig. 2에 나타내었다. Backplane 보드를 제외한 각 보드들은 이중화를 위해 2장으로 구성되어 있다. Uplink/1553B 보드는 1,024 bps의 데이터 속도를 갖는 CCSDS 원격명령 포맷[5,6]의 데이터를 CMR부터 RS-422 인터페이스를 통해 받고 원격명령을 복호하고 암호화된 명령이면 3DES CFB 모드를 이용하여 암호 복호화된다. 마이크로컨트롤러 UT80C196KDS에 의해 복호된 명령을 처리한다. SCC 명령의 경우는 SCC 명령 디코더에 의해 복호 후 보드내의 내부 로직을 제어하는 Logic-Level 형태의 명령 수행과 Backplane 보드를 통해 Command 보드에 전달되어 릴레이구동(Relay Driver) 혹은 Bilevel 형태의 구동회로를 구동한다. BUS 명령의 경우는 마이크로컨트롤러, 공유메모리 및 1553B간의 중재(Arbitration) 로직에 의해 1553B 통신을 통해 OBC에 버스 명령을 전달한다. 또한 OBC로부터 1553B 버스에 의해 받은 텔레메트리를 Backplane 보드를 통해 Telemetry 보드에 전달한다.

Telemetry 보드는 Uplink/1553B 보드를 통해 받은 2 가지 종류의 텔레메트리, 즉 Normal/Auxiliary 텔레메트리를 CCSDS 텔레메트리[7] 마이너 프레임(Minor Frame) 단위로 포맷하여 마이너 프레임당 2,048 bps의 데이터 속도로 비콘송신기에 RS-422 접속을 통해 전달한다. 메이저 프레임(Major Frame)은 40개의 마이너 프레임으로 구성된다.

Command 보드는 Uplink/1553B 보드에 의해 디코딩된 SCC 명령을 받아 Bilevel 구동 및 RD(Relay Driver) 구동을 통해 위성체의 구성을 직접제어하는 구동회로들로 구성된다.

2.2 3DES CFB 타이밍 시뮬레이션

원격측정명령처리기 성능검증모델에 적용된 3DES

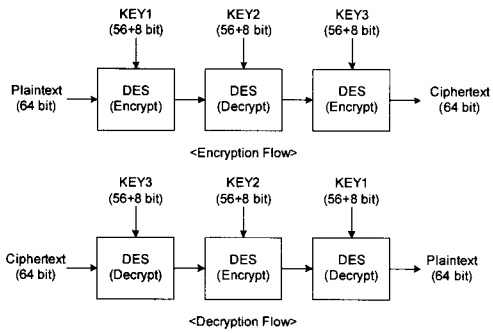

Fig. 3. Encryption/Decryption Flow of 3DES

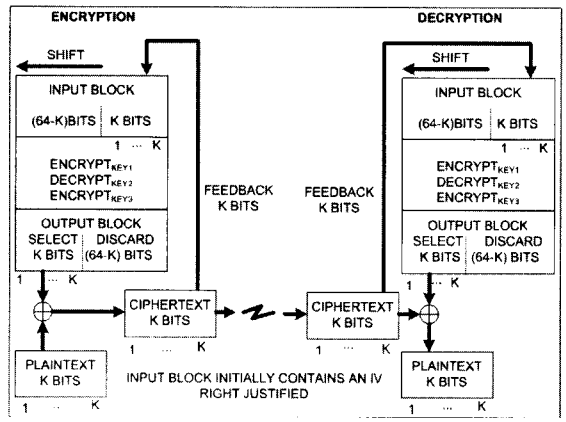

Fig. 4. Encryption/Decryption of 3DES CFB Mode

알고리즘의 암호화 및 복호화의 과정을 Fig. 3에 나타내었다. 먼저 64 비트 평문(Plaintext)에 대해 KEY1을 사용하여 DES 알고리즘으로 암호화하고 그 결과는 KEY2를 사용하여 DES 알고리즘으로 복호화하고 그 결과는 KEY3로 DES 알고리즘으로 암호화하여 최종 64 비트 암호화문(Ciphertext)을 만들어 낸다. 여기서 실제 사용되는 키의 길이는 56 비트이며 8 비트는 패리티 체크를 위해 사용된다. 복호화의 과정은 암호화 과정의 정반대로 수행되며 암호화문을 받아 평문을 만들어내게 된다.

3DES CFB 모드 암호/복호화 과정을 Fig. 4에 나타내었다[8]. CFB모드는 특성상 암호화 및 복호화 과정에서 3DES 암호화만을 사용하며 K는 평문의 데이터 길이를 나타낸다. 성능검증모델의 암호화된 CCSDS 원격명령 CLTU(Command Link Transmission Unit) 포맷[5]의 상세한 구성을 Fig. 5에 나타내었다. CCSDS 원격명령 코드블록 단위는 64 비트(데이터 56 비트 + 에러체크코드 8 비트)로 구성됨을 알 수가 있으며 당연히 평문 데이터의 길이 K는 56 비트가 되며 암호문

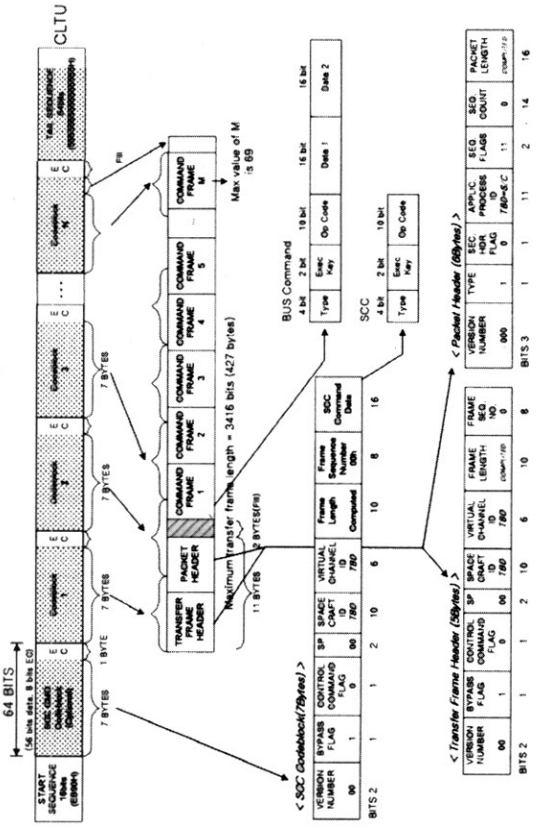

Fig. 5. Encrypted CCSDS Telecommand Format

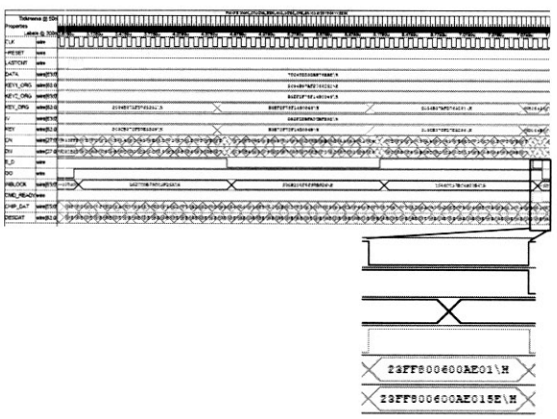

Fig. 6. Timing Simulation of 3DES CFB

의 피드백 단위도 56비트가 된다.

Fig. 5를 보면 64 비트로 구성된 코드블록의 데이터 부분인 56 비트에 대해서만 DES CFB 모드로 암호화하고 나머지 EC 코드 8 비트는 암호화되지 않는다. 또한 후미 시퀀스도 64 비트 중 56 비트만 암호화된다. 단지 시작 시퀀스 16 비트만이 암호화되지 않는다.

3DES에서 3 개의 키들을 사용하는 3가지 방법이 있다. KEY1, KEY2, KEY3를 각각 다르게 사용하는 경우와 KEY1과 KEY2는 다르게 사용하고 KEY3와 KEY1는 같게 사용하는 경우와 KEY1, KEY2, KEY3를 같이 사용하는 경우가 있다. KEY1/2/3를 각각 다르게 사용하는 첫 번째의 경우는 각 키들을 저장할 공간이 크게 증가하게 된다. 그래서 보안성 강화 및 메모리 사용의 최소화를 위해 두 번째 경우에 해당하는 KEY1= KEY3≠KEY2를 선택하였다.

Fig. 6에 3DES CFB 암호 복호화 과정 타이밍 시뮬레이션 파형을 나타내었다. Viewdraw/ Viewsim 7.3을 사용하여 실험모델에서 검증된 DES CFB 코어를 기반으로 하여 3DES CFB코어를 확장하여 설계하고 타이밍 시뮬레이션을 통해 검증한 뒤, 다중 암호화 키 및 IV 값을 ACC와 배타적논리합하여 새로운 암호화 키 및 IV를 생성하는 로직을 추가하여 만든 최종 Netlist를 Actel Designer Series 5.0에서 Fuse 파일을 만들고 Silicon Sculptor를 통해 Actel A54SX32 FPGA에 Fusing하였다.

여기서 사용된 데이터는 SCC 명령중 OBC 1 On에 해당하는 코드블록을 선정하여 복호화 타이밍 시뮬레이션을 하였다. 아래에 3DES CFB 암호화된 암호문에 KEY1/2 및 IV에 ACC를 적용하고 3DES CFB 복호화 시뮬레이션을 통해 얻은 평문을 나타내었다.

암호문 : 0x7DC4DDD3DBB76E5E
KEY1 : 0x2034B37AFD763231
KEY2 : 0xB3EF2F75F1450843
IV : 0xD52FCDBFADCBF292
ACC : 8
평문 : 0x23FF800600AE015E

타이밍 시뮬레이션을 통해 얻어진 평문은 C++ 소프트웨어 실행결과와 비교하였고 동일한 결과를 얻을 수 있었다.

2.3 다중 키/IV 활용 및 명령 재공격 보안

단일키 및 단일 IV를 사용할 경우 간편하지만 위성 키 및 IV가 해킹될 경우 위성에 치명적 영향을 막기 위해 지상 명령에 의해 다중 키 및 IV를 변경하여 사용할 수 있도록 하였다. 이를 위해 이미 실험모델에서 다중 키 및 IV에 대한 Key 및 IV 인덱스(Index) 개념을 적용하여 복호화 키 변경 기능을 제공하도록 하였다[3]. Table.

1에 원격측정명령처리기 성능검증모델의 Key1/2 및 IV Index 테이블을 보여주고 있다.

Table 1. Key1/2 and IV Index Table

Key1 Indexes	Notes
0-31	Valid Indexes
32-63	Repeat of Key1s 0-31
Key2 Indexes	Notes
0-31	Valid Indexes
32-63	Repeat of Key2s 0-31
IV Indexes	Notes
0-31	Valid Indexes
32-63	Repeat of IVs 0-31

원격측정명령처리기 실험모델에서 FPGA 내부에 키 및 IV를 저장하였으나 성능검증모델에서는 KEY 개수가 2 배로 증가하면서 외부에 PROM을 장착하여 KEY1, KEY2 및 IV를 저장하여 SCC 명령인 KEY1/2 및 IV INDX CHANGE 명령을 수행하여 복호화 키 및 IV 변경을 수행하도록 하였다. KEY1/2 Index 32~63은 KEY1/2 Index 0~31의 KEY1/2 값에 대한 중복으로 설정되어 메모리 오류로 인한 KEY1/2 손실을 극복할 수 있도록 하였다.

원격측정명령처리기 실험모델에서 제안되었던 원격명령 재공격을 막기 위해 위성에서 원격명령 암호복호 인증시 16 비트의 ACC 카운터 값을

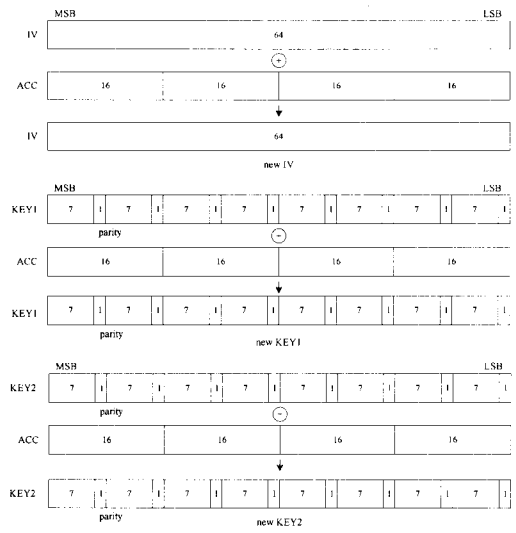

Fig. 7. New Key1/2 & IV Generation Flow by Exclusive-OR with ACC

증가시키도록 하였다[3]. 성능검증모델에서는 KEY1 및 KEY2를 사용하기 때문에 Fig. 7에 ACC와 배타적논리합을 적용하여 새로운 KEY1, KEY2 및 IV를 생성하는 구조를 나타내었다. 64 bit IV 및 64 bit KEY1/2(56 비트 키 + 8 비트 패리티)를 현재의 ACC와 배타적논리합(Exclusive-Or) 연산을 통해 새로이 생성된 KEY1/2 및 IV는 3DES CFB 로직의 입력으로 사용된다. 위성에서 하나의 원격명령이 인증되면 ACC 값은 증가되고, 이 증가된 ACC는 지상국에 Normal Telemetry로 전송된다. 지상국에서는 받은 ACC를 가지고 같은 방법으로 새로운 IV 및 KEY1/2를 생성하여 원격명령 데이터를 암호화한 후 업링크한다.

원격측정명령처리기 성능검증모델에서는 3DES로 인한 키 개수의 증가에 따라 KEY1 및 KEY2의 Index를 텔레메트리로 받는 것과 KEY1 및 KEY2 Index Change 명령을 추가하여 운용하도록 하였다.

2.4 원격명령 암호화 처리 운용

Fig. 8에 위성과 지상국 간의 암호화 운용 과정을 보여주고 있다. 원격명령 암호화 처리 과정을 설명하면 다음과 같다.

(가) 지상국 초기 설정

① 위성체로부터 암호화 Key1/2 Index 및 IV Index를 Normal 텔레메트리로 수신
② 지상국을 Normal 텔레메트리로 받은 것과 같은 Key1/2 및 IV Index로 설정
③ ACC 비트를 Normal 텔레메트리로 받고 같은 값으로 설정
④ 암호문모드(Encrypted Mode)로 설정

(나) 위성체 암호화 모드 설정

① Uplink Decryption On 명령 전송
② Decrypt Mode=1(On) 상태를 Normal 텔레메트리로 수신

(다) 암호화된 명령 전송

① 지상국에서 Normal 텔레메트리로 받은 Key1/2 및 IV Index에 해당하는 Key1/2 및 IV와 ACC를 Exclusive-OR하여 새로운 Key1/2 및 IV 값을 생성
② 평문모드(Clear Mode) 명령을 생성
③ 평문모드 명령을 새로 생성된 Key1/2 및 IV로 암호화
④ 암호화된 명령을 위성체에 전송
⑤ 위성체에서는 받은 암호화된 명령을 현재의 Key1/2 및 IV와 ACC를 배타적논리합하여 생성된 Key1/2 및 IV를 이용하여 암호 복호화를 수행하고 인증시 ACC 카운터 값을 1 증가

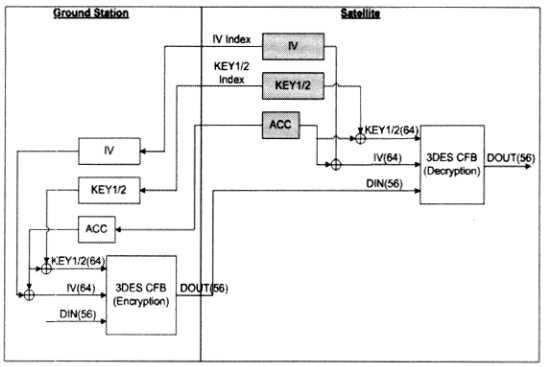

Fig. 8. Encryption/Decryption Operation Flow between Satellite and Ground Station

⑥ Decrypt Mode, Key1/2 Index, IV Index 및 ACC를 텔레메트리로 전송받고 상태를 확인

⑦ 암호문모드를 계속하려면 ①에서 재시작하고 암호문모드를 종료하려면 Decryption Off 명령을 전송

(라) Key1/2 및 IV Index 변경

① Key1/2 INDX CHANGE 및 IV INDX CHANGE 명령 전송

② Key1/2 및 IV Index Change 명령에 의해 위성체의 암호화 Key1/2 및 IV를 변경

③ 바뀐 새로운 Key1/2 및 IV Index를 Normal 텔레메트리로 수신

2.5 3DES CFB 원격명령 복호화 성능 시험 결과

성능검증모델의 3DES 원격명령 복호화 처리 및 인증을 행하고 1553B 통신을 통한 명령 전달 및 텔레메트리 수집을 하는 Uplink/1553B 보드 외형과 Uplink/1553B 보드와 나머지 보드들을 함께 하우징에 장착한 원격측정명령처리기 성능검증모델 외관을 Fig. 9에 보여주고 있다.

Fig. 10은 원격명령 암호 복호화 및 명령 전송을 시험하기 위해 구축된 시험 환경을 보여준다. 소프트웨어적으로 원격명령을 생성하고 성능검증모델의 텔레메트리를 모니터링하는 PC, PC로부터 RS-422 통신으로 원격명령을 받아 성능검증모델로 전송하고 성능검증모델에서 전송되는 텔레메트리를 받아 모니터링 PC에 전달하는 TCTS (Telemtry Command Test Set), TCTS에서 RS-422 통신으로 받은 원격명령을 암호 복호화한 후 SCC 명령이면 Relay 및 Bilevel 구동 명령을 TCTS에 전달하고 그 상태를 TCTS 전면 패널에 있는 LED의 On/Off로 확인하도록 하고 Bus 명령이면 1553B 버스를 통해 OBC에 전달하는 기

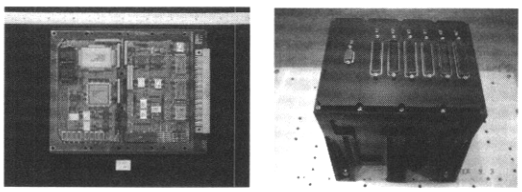

Fig. 9. Uplink/1553B Board and CTU EQM

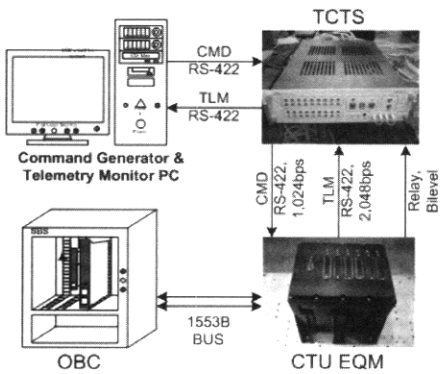

Fig. 10. Functional Test Bed of CTU EQM

능을 하는 성능검증모델 및 성능검증모델로부터 1553B 통신에 의해 받은 Bus 명령을 처리하는 기능과 수집된 SOH 데이터를 1553B 데이터버스를 통해 성능검증모델에 전송하는 OBC로 구성된다.

성능검증모델의 원격명령 처리 성능 검증을 위해 SCC 명령 및 버스 명령 각각에 대해 평문모드(Clear Mode) 전송 및 암호문모드(Encrypted Mode) 전송으로 나누어 시험을 수행하였다. SCC 명령 검증을 위해 여러 개의 SCC 명령들 중에 타이밍 시뮬레이션에 사용되었던 OBC1 ON에 해당하는 코드블록을 사용하여 기능 시험을 하였다. 명령 생성 PC에서 SCC 명령 생성의 용이함을 위해 Fig. 11과 같은 GUI 화면을 만들었다.

Fig. 11은 SCC 명령 OBC1 ON을 생성하는 GUI 화면을 보여주고 있다. Fig. 5에 보인대로 SCC 명령 데이터(16 비트)는 명령 타입(4 비트), 실행여부(2 비트) 및 수행코드(10 비트)로 구성된다. OBC1 ON에 해당하는 각 타입, 실행여부 및 수행코드를 설정하고 'Send' 아이콘을 클릭하면 0xAE01이라는 SCC 명령 데이터가 생성되고 0xAE01에 트랜스퍼 프레임 헤드 정보 0x23FF800600를 붙인 후 BCH 에러체크 후 얻은 5E를 붙여 64비트(8바이트) 코드블록을 생성한 후에 시작시퀀스 0xEB90 및 후미시퀀스 0x5555555555555555를 자

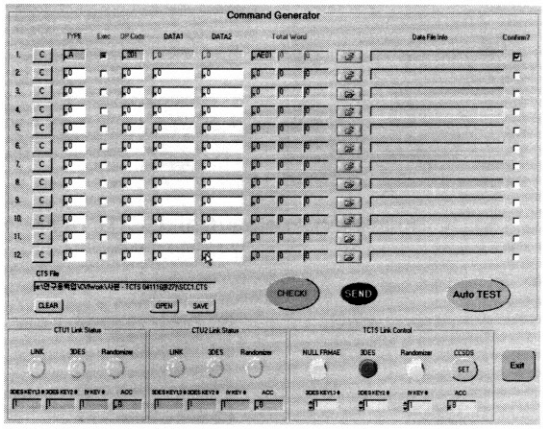

Fig. 11. GUI of SCC Command Generator

동으로 생성하여 붙여 평문모드 전송데이터(0xEB90 23FF800600AE015E 5555555555555555)가 만들어진다. 그후 만들어진 평문모드 전송데이터는 TCTS를 거쳐 성능검증모델에 전달되고, 성능검증모델에서는 0x23FF800600AE015E가 얻어지고 SCC 디코더에 의해 수행코드에 해당하는 0xAE01가 디코딩되면 22±4ms의 구동 펄스 신호가 Backplane 보드를 통해 Command 보드의 Bilevel 구동 회로를 구동하고 구동된 신호는 TCTS에 전달되고 TCTS의 전면에 있는 LED를 On하는 것을 확인하였다.

암호문모드 전송의 경우는 평문모드 전송 데이터에 타이밍 시뮬레이션에 사용된 것과 동일한 Key1/2, IV 및 ACC를 설정하고 '3DES' 아이콘을 클릭하면 0xEB90을 제외한 평문 전송데이터에 대해 3DES CFB 암호화를 한 후 암호문모드 코드블록 데이터가 생성되고 'Send' 아이콘을 클릭하면 암호문모드 전송데이터(0xEB90 7DC4DDD3DBB76E5E760391D12770CF55)가 TCTS를 거쳐 성능검증모델에 전달되고 암호 복호화된다. 암호 복호화가 되면 나머지 과정은 평문모드에서 설명한 과정과 동일하다. 원격명령 복호가 검증되면 코드블록 단위로 ACC가 증가되고 그 값은 Normal 텔레메트리로 모니터링 PC로 전달된다. 명령 생성 PC는 그것을 받아 다음 원격 명령을 암호화하는데 사용한다.

나머지 SCC 명령들도 동일한 전송시험을 통해 모두 정상적으로 동작함을 확인하였다.

버스 명령에 대해서도 SCC 원격명령의 전송시험의 경우처럼 평문모드 및 암호문모드로 나누고 버스 명령 전송시험을 수행하였다. Fig. 5에 보인 대로 버스 명령 프레임 길이(48 비트)는 명령타입(4 비트), 실행여부(2 비트), 수행코드(10 비트), 데이터 1(16 비트) 및 데이터 2(16 비트)로 구성된다. Fig. 12에 버스 명령 생성 GUI 화면을 나타내었다.

먼저 평문모드 버스 명령 전송시험의 한 예로 명령타입, 실행여부, 수행코드, 데이터1/2를 입력하고 'Send' 아이콘 클릭한 후 최종 생성된 전송데이터는 다음과 같다.

-0xEB90 23FFFC06000000FA
0000000003021DB2 BF123445670000DC
5555555555555555

이 데이터는 TCTS를 거쳐 성능검증모델에 전송되고 원격명령 처리 후 1553B 통신을 통해 OBC에 전달되고 명령생성 PC에서 생성한 버스 명령 프레임과 받은 버스 명령 비교를 하여 동일함을 확인하였다.

암호문모드 버스 명령 전송의 경우는 평문모드 전송 데이터에 다음과 같은 Key1/2, IV 및 ACC를 설정한다.

-KEY1 : 0x2034B37AFD763231
-KEY2 : 0xB3EF2F75F1450843
-IV : 0x6B9BB03745EC4661
-ACC : 0

'3DES' 아이콘을 클릭하면 0xEB90을 제외한 평문 전송데이터에 대해 3DES CFB 암호화를 한 후 다음과 같은 암호문모드 버스 명령 전송데이터가 생성된다.

-0xEB90 65933B039DB3A2FA
BDFCFC827AAD62B2 85A402C7F8A339DC
C47D947E3A90BF55

'Send' 아이콘을 클릭하면 성능검증모델에 전송되고 암호 복호화가 된다. 그 다음 과정은 평문모드의 경우와 동일한 과정으로 검증된다. 원격명령 복호가 검증되면 코드블록 단위로 ACC

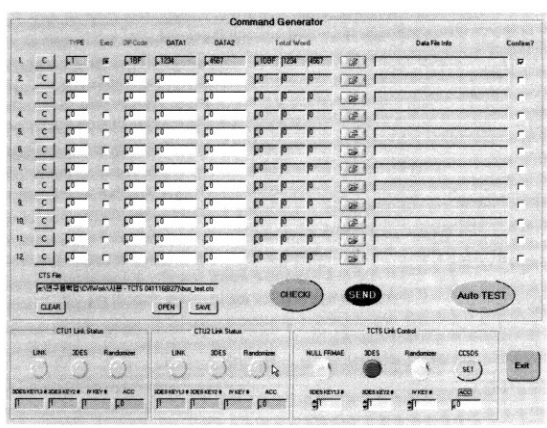

Fig. 12. GUI of BUS Command Generator

가 증가하고 Normal 텔레메트리로 모니터링 PC에 전달되고 다음 원격 명령을 암호화하는데 사용된다.

또한 Key1/2 및 IV Index Change 명령도 전송하여 Key1/2 및 IV Index를 변경하고 그것을 Normal 텔레메트리로 받아 명령 생성 PC에서 받은 Index 값들을 사용하여 새로운 원격명령을 생성하고 전송하는 시험을 앞에서 설명한 과정대로 SCC 및 버스 명령 각각에 대해 수행하였고 모두 정상적으로 동작함을 확인하였다.

III. 결 론

본 논문에서는 DES CFB 암호화 알고리즘을 사용한 원격측정명령처리기 실험모델의 경우 보다 강화된 원격명령 보안성을 제공하기 위해 3개의 키를 사용하는 3DES CFB 알고리즘을 원격측정명령처리기 성능검증모델에 구현하고 검증하였다. 3DES 알고리즘에 따른 증가된 KEY와 IV를 위해 외부에 PROM을 두도록 하고 설정된 Index에 대한 키 및 IV를 가져와서 복호화 하도록 하였다. 설계된 3DES CFB 코어의 타이밍 시뮬레이션을 통해 동작 검증 후 Actel사의 A54SX32 FPGA에 구현하였다. 원격명령 암호 복호화 기능 검증을 위한 시험환경을 구축하고 원격측정명령처리기 성능검증모델에 원격명령 전송, 암호 복호화 후 수행코드 모니터링 및 수행에 의한 LED On/Off 확인을 통해 3DES CFB 원격명령 복호화 기능을 검증하였다. 본 연구결과는 향후 국내의 저궤도 및 정지궤도 위성의 CCSDS 원격명령 암호화 구현에 직접 적용될 수 있다고 사료된다.

후 기

본 연구는 과학기술부의 IMT-2000 기술 개발 지원 사업의 일환으로 수행되었으며 연구비 지원에 감사드립니다.

참고문헌

1) FIPS PUB 81, DES Modes of Operation, Dec. 1980.

2) 김중표, 구철회, 최재동, "정지궤도 통신위성의 CCSDS 원격명령 암호복호기 구현", 한국항공우주학회지, 제 31권, 제 10호, 2003, pp. 89-96.

3) 김중표, 구철회, "통신위성 원격측정명령처리기 실험모델 암호화 연구", 한국항공우주학회 춘계학술발표회 논문집, 2004, pp.980-983.

4) CCSDS 350.0-G-1 The Application of CCSDS Protocols to Secure Systems, March 1992.

5) CCSDS 202.0-B-2 Telecommand Part 1 - Data Routing Service, Nov. 1992.

6) CCSDS 201.0-B-1 Consultative Committee for Space Data Systems Telecommand Part 1 - Channel Service, Jan. 1987.

7) CCSDS 102.0-B-3, Packet Telemetry, Nov. 1992.

8) NIST Special PUB 800-20, Modes of Operation Validation System for the Triple Data Encryption Algorithm(TMOVS): Requirements and Procedures, April 2000.