갈릴레오 시스템과 연동한 COSPAS-SARSAT 탐색구조 신호 보안

조태남*, 백유진*ⓒ, 김재현**, 이상욱** 정회원, 안우근***

Securing COSPAS-SARSAT Search-and-Rescue Signal with Galileo System

Taenam Cho*, Yoojin Baek*ⓒ, Jaehyun Kim**, Sanguk Lee** *Regular Members* and Woo-Geun Ahn***

요 약

COSPAS-SARSAT 탐색구조 시스템을 이용하여 조난을 당한 비행기, 선박 혹은 개인은 구조 기관에 구조신호를 송신함으로써 구조를 받을 수 있다. 특히 이러한 시스템이 전시에 사용될 경우, 조난신호의 노출은 조난자의 위험과 지원 자원의 낭비를 초래할 수 있다. 본 논문에서는 COSPAS-SARSAT을 탐색구조 신호를 보호하기 위한 개선된 방안을 제안한다. 또한 갈릴레오 시스템의 탐색구조 회신링크를 이용하여 조난자와 구조 기관간의 안정된 보안 체계를 유지할 수 있는 프로토콜을 제안한다.

Key Words : SAR, Security, COSPAS-SARSAT, Galileo

ABSTRACT

The COSPAS-SARSAT Search-and-Rescue System detects and locates emergency beacons activated by aircraft, ships and individuals. In particular, when this system is used in wartime and the signal is leaked to the enemy, it can cause the loss of the rescuers and the survivors. This paper proposes an improved method which protects the COSPAS-SARSAT search-and-rescue signal itself from being disclosed during its operation. In addition, there is presented a new protocol which maintains the stabilized security status between survivors and rescuers, using the Galileo/SAR return link.

I. 서 론

위성을 통한 탐색구조 시스템은 비행기나 선박, 개인이 조난을 당했을 때 각각 ELT(Emergency Locator Transmitters), EPIRB(Emergency Position-Indicating Radio Beacon), PLB(Personal Locator Beacons)라고 불리는 탐색구조 단말기를 이용하여 자동 혹은 수동으로 조난 위치가 포함된 구조신호를 위성으로 보내는 방식을 사용한다. 이 때 지역수신지구국(LUT : Local User Terminal)은 위성이 중계한 신호를 받아 임무통제본부(MCC: Mission Control Center)로 전송하고, MCC에서는 구조조정본부(RCC: Rescue Control Center)로 구조를 요청하게 된다(그림 1 참조).

특히 전시에 군인이 조난을 당하거나 중요한 사람, 물건

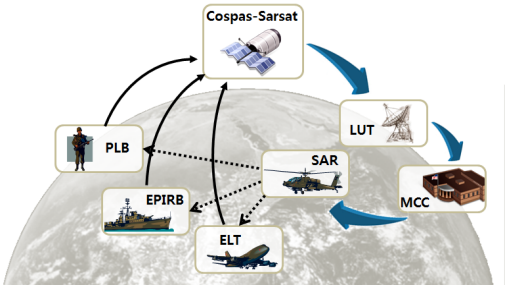

그림 1. COSPAS-SARSAT 탐색구조 시스템[1]

혹은 정보가 포함된 비행기가 불시착하거나 선박에 조난이 발생하는 경우 이들이 보내는 비상 탐색구조신호가 적군이나 이를 악용할 제 3자에게 노출된다면 심각한 결과를 초래할 수 있다. 또한 탐색구조를 지연시키거나 방해할 목적으로 탐색구조시스템을 교란시킨다면 적시에 구조가 이루어지지

※ 본 연구는 방위사업청과 국방과학연구소가 지원하는 국방위성항법 특화연구센터 사업의 일환으로 수행되었음.
*우석대학교 정보보안학과 (tncho@ws.ac.kr, yjbaek@ws.ac.kr), **한국전자통신연구원 위성무선융합연구부(longinus@etri.re.kr, slee@etri.re.kr),
***국방과학연구소 제3기술연구본부(wgahn@add.re.kr)
접수일자 : 2014년 12월 3일, 수정완료일자 : 2014년 12월 24일, 최종게재확정일자 : 2014년 12월 24일

표 1. COSPAS-SARSAT 장문 메시지 포맷

비트 번호	1 15	16 24	25 85				86 106	107 132	133 144
필드	15	9	61				21	26	12
	Bit Synch.	Frame Synch.	First Protected Data Field (PDF-1)				BCH-1	Second Protected Data Field (PDF-2)	BCH-2
서브필드/데이터	Bit Synch. Pattern	Frame Synch. Pattern	1	1	10	49	Error Corr. Code for PDF1	Supplementary and Position or National Use Data	Error Corr. Code for PDF2
			Format Flag	Protocol Flag	Country Code	Identification or Identification plus Position			

않거나 인력이나 자원의 낭비 및 혼란을 초래할 수 있다.

COSPAS-SARSAT은 위성 기반의 조난 탐색 및 구조 시스템으로서 1979년에 캐나다, 프랑스, 미국 및 구소련에 의해 처음 설립되었고 현재 대한민국을 포함한 43개 국가가 참여하고 있으며, 항공기나 선박 등에 의해 활성화된 탐색구조 신호를 탐지하고 그 위치를 특정할 수 있는 시스템으로 잘 알려져 있다[1]. 반면에 갈릴레오 위성 시스템은 전 세계적으로 제공되는 3개의 위성항법시스템 중의 하나이며 유럽 우주국(ESA) 및 타 국가들이 공동으로 개발하고 있는 최초의 민간용 범지구 위성항법시스템으로서 우리나라도 이 프로젝트에 참여하고 있다[2].

3대 위성항법시스템 중의 하나인 GPS에 대한 보안 시스템도 운용되고 있으나, 미군에서만 사용하고 이를 적용한 완제품만 사용할 수 있기 때문에 우리 환경을 반영하기 어려우며, 완제품을 그대로 우리나라에 적용할 경우 막대한 비용이 수반된다.

본 논문에서는 COSPAS-SARSAT의 기본 구조를 유지하면서 탐색구조 신호를 보호하기 위한 개선된 방안과 갈릴레오 탐색구조시스템의 회신링크를 이용한 조난자와 구조기관간의 안정된 보안 체계를 유지할 수 있는 프로토콜을 제안한다. COSPAS-SARSAT의 탐색구조신호를 보호하기 위한 보안 방안이 이전에도 연구된 바 있으나, 이 방식의 안전한 구현을 위해서는 송수신자간의 동기화가 필수적이기 때문에 새로 제안하는 방식은 사용된 암호알고리즘에 대한 안전한 키관리 프로토콜과 이를 고려한 개선된 탐색구조 신호 메시지를 설계하였다.

본 논문의 구성은 다음과 같다. 먼저 2장과 3장에서는 COSPAS-SARSAT시스템과 갈릴레오 위성 시스템에 대한 간단한 소개를 하고 4장에서는 개선된 COSPAS-SARSAT 탐색구조 신호 보안 방안과 갈릴레오 위성을 이용한 키관리 방안을 제안한다. 마지막으로 5장에서는 제안한 방식의 제한사항과 결론을 기술한다.

Ⅱ. COSPAS-SARSAT 위성 통신망 서비스 분석[3]

COSPAS-SARSAT 탐색구조(Search and Rescue) 시스템에서 조난자의 위치를 추적하고 해당 선박이나 항공기, 조난자를 식별하기 위해서 사용되는 메시지 포맷은 COSPAS-SARSAT 관리문서 형식으로 사무국에서 관리되고 있다. 본 장에서는 보안 방안 도출을 위해 COSPAS-SARSAT의 탐색구조 신호 메시지 포맷을 분석한다.

1. 기본 메시지 포맷

메시지는 112비트의 단문과 144비트의 장문을 지원하고 있다. 단문 형태는 초창기 단말기를 위한 포맷이고, GPS 정보를 같이 송신할 수 있는 단말기가 사용됨에 따라 위치 정확도를 높이기 위하여 두 번째 데이터 영역을 추가한 장문 형태가 개발되었다. 본 연구에서 위치정보의 정보의 정확도와 보안성을 높일 수 있는 장문 메시지 포맷을 이용하므로 장문 메시지를 중심으로 기술한다. 표 1은 장문 메시지 포맷에 따른 구조신호의 데이터 필드를 보여준다.

장문 메시지 포맷의 데이터 필드가 담고 있는 정보는 표 2와 같다. 수신자가 비트와 프레임 동기화 비트는 신호와 메시지의 시작점을 인식할 수 있도록 하는 상수값이다. 포맷과 프로토콜 플래그는 나머지 영역의 구조를 정의하는 필드로서 표 3과 같이 정의된다. 탐색구조 단말기의 식별자는 보편적으로 해상이동업무용 식별부호 (MMSI: Maritime Mobile Service Identity)가 사용되며, 국가 코드는 비컨이 등록된 국가를 의미한다. Protected Data Field-1(PDF-1)의 37-85비트와 PDF-2의 107-132비트 영역에는 실제 데이터가 들어가는 부분으로서, 사용하는 프로토콜에 따라 세부 포맷이 다르다 (표 3참조). 86-106비트는 PDF-1영역에 대한 데이터 통신 에러를 정정하기 위한 코드 삽입용으로 사용되며, 사용되는 에러정정코드는 BCH (Bose-Chaudhuri-Hocquenghem) 코드이다. 133-144비트는 PDF-2영역에 대한 데이터 통신 에러를 정정하기 위한 BCH 코드용으로 사용된다.

표 2. 메시지 필드의 정보

필드명	정 보
Bit Synch.	비트 동기. 111111111111111(2)
Frame Synch.	프레임 동기 비트. 2가지 모드로 운용 - normal op. mode: 000101111(2) - self-test mode: 011010000(2)
Format Flag	메시지의 단문/장문 형태 구분. 0: 단문, 1: 장문
Protocol Flag	COSPAS-SARSAT 위성 통신망 서비스가 사용하는 프로토콜의 종류
Country Code	국가코드. 우리나라는 440(10) = 0110111000(2) 또는 441(10) = 0110111001(2)
ID or ID+Position	실제 데이터 부분으로서 사용하는 프로토콜에 따라 다르며, 단말기 식별자나 위치 정보를 포함
BCH-1	PDF-1에 대한 BCH 에러 정정 코드
Suppl. Pos. or National Use Data	부가적 위치정보나 국가 사용 데이터를 포함
BCH-2	PDF-2에 대한 BCH 에러 정정 코드

표 3. 포맷 플래그와 프로토콜 플래그에 따른 프로토콜 종류

Format Flag / Protocol Flag	0 (단문 메시지)	1 (장문 메시지)
0	사용 안함	표준 위치 프로토콜 국가 위치 프로토콜 RLS 위치 프로토콜
1	사용자 프로토콜	사용자 프로토콜 사용자 위치 프로토콜

2. 위치정보 인코딩

COSPAS-SARSAT 단말기는 위치정보를 PDF-1과 PDF-2에 인코딩한다. PDF-1의 37-85비트 영역은 표 5와 같이 정의된다. 예로 위도의 경우, NS=$0_{(2)}$, 도(Degrees) = $0010010_{(2)}$ = $18_{(10)}$, 분(Minutes) = $11001_{(2)}$ = $25_{(10)}$ 라면, 이것은 북위 18도 50분을 나타낸다. 경도의 경우에도 이와 유사하게 인코딩 된다. PDF-2의 107-132비트 영역은 표 6과 같이 정의되며, 위치 정보는 PDF-1의 위치정보를 보정하는 데이터이다. 만약 △위도(Latitude) 필드값이 $1010101_{(2)}$라면 PDF-1 위도 좌표에 1분 5×4=20초를 빼서 보정해야 하므로, 실제 위도값은 북위 18도 48분 40초이다. △경도(Longitude)도 동일한 방법으로 반영된다.

표 5. PDF-1의 위치 정보

비트 길이		필드		용도 / 값
4		프로토콜 코드		ELT=1000, EPIRB=1010, PLB=1011
18		비콘 식별자		비콘 식별자
13	1	위도	NS	0: 북위, 1: 남위
	7		Deg	0-90도. 정밀도: 1도
	5		Min	0-58분. 정밀도: 2분
14	1	경도	EW	0: 동경, 1: 서경
	8		Deg	0-90도. 정밀도: 1도
	5		Min	0-58분. 정밀도: 2분

표 6. PDF-2의 위치 보정 정보

비트 길이		필드		용도 / 값
6		보조 데이터		위치정보 제공 장치 정보 등
7	1	△ Latitude (위도 오프셋)	Sign	0: -, 1: +
	2		Min	0-3분. 정밀도: 1분
	4		Sec	0-56초. 정밀도: 4초
7	1	△ Longitude (경도 오프셋)	Sign	0: -, 1: +
	2		Min	0-3분. 정밀도: 1분
	4		Sec	0-56초. 정밀도: 4초
6		국가 용도		국가별로 정의

Ⅲ. 갈릴레오(Galileo) 위성 통신망 서비스 분석

본 장에서는 COSPAS-SARSAT과 연계하여 운영하고자 하는 갈릴레오 시스템에 대해 기술한다.

1. 갈릴레오 시스템 사용 현황

갈릴레오 시스템은 GPS, 글로나스(Glonass), Beidou와 같은 위성항법시스템 중의 하나로서 기존 시스템과 달리 회신링크(Return Link) 서비스 도입을 선언하여 COSPAS-SARSAT 시스템과 긴밀한 연계관계를 가지고 있다. 현재 COSPAS-SARSAT 시스템은 저궤도 탐색구조 시스템(LEOSAR)과 정지궤도 탐색구조(GEOSAR) 시스템을 운용

표 4. 국가 위치 프로토콜 메시지 포맷

필드	61												21	26											12
	First Protected Data Field (PDF-1)												BCH-1	Second Protected Data Field (PDF-2)											BCH-2
	1	1	10	4	18	27								6	14									6	
						Latitude			Longitude						△Latitude			△ Longitude							
서브 필드/ 데이터	Fmt Flag =1	Prot. Flag =0	Countnry Code =440(10)	Prot. Code =1000, 1010, 1011	National Id (Beacon Id)	1	7	5	1	8	5		Error Corr. Code for PDF1	Suppl. Data	1	2	4	1	2	4					Nat-ional Use (Cnt)	Error Corr. Code for PDF2
						NS	Deg	Min	EW	Deg	Min				Sign	Min	Sec	Sign	Min	Sec					

중이다(그림 2 참조)[7]. 저궤도 탐색구조 시스템은 도플러 기술을 이용해 전지구를 서비스하지만 탐색시간과 위치 커버리지가 불연속적이며, 이러한 불연속적 커버리지 때문에 조난신호 전달에 지연이 생길 수 있다. 정지궤도 탐색구조 시스템은 정지궤도 위성에 의해 거의 즉각적인 조난신호 전달을 제공할 수 있지만 낮은 앙각으로 인하여 실제 운용에 애로사항이 많은 상태이다. 이를 극복하기 위하여 COSPAS-SARSAT 위원회에서는 기존 저궤도 탐색구조를 대체할 새로운 탐색구조 시스템으로 중궤도 위성을 이용한 탐색구조 시스템(MEOSAR)을 구축하고 있다. 이러한 중궤도 탐색구조 시스템은 이전 두 시스템의 장점을 가진 전지구 실시간 탐색구조 서비스를 제공할 수 있을 것으로 기대되고 있다. 갈릴레오 시스템에서의 탐색구조 서비스(SAR/Galileo)는 COSPAS-SARSAT 시스템의 지상부문(MCCs, RCCs, MEOLUTs 와 RLSP)과 우주부분(Satellite, SAR Transponder)으로 구성된다[2,4,5,6].

현재 중궤도 탐색구조 시스템의 경우 GPS, 갈릴레오, 글로나스 위성에 탐색구조 탑재체를 탑재하고 있으며, 이중 갈릴레오, 글로나스 시스템에서 회신링크 서비스를 제공할 예정이다. 글로나스의 경우 현재 계획 단계이며, 실제 회신링크 서비스 제공은 갈릴레오 시스템을 통하여 가능하므로, 그림 2에서와 같이 갈릴레오 회신링크 서비스를 연계하여 활용하고자 한다.

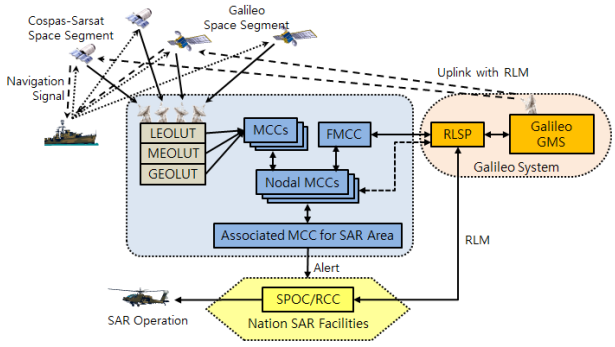

그림 2. COSPAS-SARSAT과 Galileo를 연계한 회신링크 서비스[7]

2. 회신 링크 메시지(RLM: Return Link Message) 구조[7,8,9,10]

회신링크 서비스와 Cospass-Sarsat과의 통합에 대한 논의가 최근 2년 동안 이루어졌으며, 상세한 규격은 아직도 논의 중에 있다.

RLM(Return link Message)은 80비트 단문 혹은 160비트 장문 메시지로 이루어진다. 본 절에서는 보안 방안에 활용될 수 있는 장문을 기술한다. 장문 메시지의 필드 구성은 표 7과 같다.

표 7. 장문 RLM 메시지 포맷

비트 길이	필드	용 도
60	비컨 식별자	메시지 송수신 비컨을 구분하는 60비트 식별자로서, COSPAS-SARSAT 메시지의 26-85 비트와 동일
4	메시지 코드	파라미터 필드를 정의하는 메시지 코드 1: Acknowledgement: FLAM (Forward Link Alert Message) 수신에 대한 피드백을 주고 위치를 측정하기 위한 기본적 RLM 서비스 2: COMMAND: 비컨 활성화나 전송 파라미터 수정을 원격으로 제어 3: MESSAGE: 비컨에게 텍스트 메시지나 테이블에 미리 정의되어 있는 메시지의 참조번호를 전송 4: TEST RLS 테스트용. 테스트 기관이 정의한 메시지를 전송
95	파라미터	메시지 코드에 따라 필요한 데이터
1	패리티	1-159비트에 대한 짝수 패리티

Ⅳ. COSPAS-SARSAT의 탐색구조 신호 보안 방안 제안

1. 관련 연구[11,12]

서론에서 기술한 바와 같이 COSPAS-SARSAT의 탐색구조 신호에 포함된 위치정보는 노출되어서는 안 되며, 위치정보의 기밀성을 제공하기 위한 방안으로서 [12]가 제안되었다. 보안 서비스를 고려하지 않고 설계하여 이미 운영되고 있는 기존의 탐색구조 신호에 보안 기능을 제공하기 위해서는 여러 가지 제약점이 따른다. 가장 중요한 제약점 중의 하나는 현행의 메시지 구조를 준수해야 한다는 것이다. [12]에서는 위치 정보의 정확도가 가장 높고 자유롭게 정의하여 사용할 수 있는 필드를 포함한 국가 위치 프로토콜을[3] 이용하도록 제안하였다.

표 4는 표 1에서 고정적으로 사용되는 동기화 비트를 제외하고 25-144비트의 국가 위치 프로토콜 메시지 구조를 보여준다. 이 중 국가 식별자(National Id)는 단말기를 구분할 수 있는 비컨 식별자(Beacon Id)로 활용한다. PDF-1에 있는 경위도 좌표 정보 27비트와 PDF-2에 있는 경위도 보정 정보 14비트가 보호되어야 할 영역이다. 따라서 암호화되어야 할 비트 길이는 41비트이다. 기존의 블록암호 시스템에 적용하기에는 너무 짧은 길이이기 때문에 128비트 AES-CFB 운용모드를 제안하였다. 이 모드는 스트림 암호방식이기 때문에 송수신자간의 동기화가 매우 중요하다. 동기화 확인을 위한 방안으로서 표 4의 국가별 사용(National Use) 필드를 카운트(CNT) 필드로 사용하고 이 필드도 암호화 영역에 포함시켜서 47비트를 암호화 필드로 정의하였다.

단말기로부터 수신한 메시지를 복호화하기 위해서 MCC는 각 단말기에 대하여 공유한 비밀키, 최종 카운터, IV(Initialization Vector)를 단말기와 공유한다. 단말기로부터 메시지를 수신하면 BCH-1과 BCH-2를 통해 오류를 정정한한 후, 비컨 아이디로부터 복호화할 키를 결정하여 메시지를 복호화한다. 만약 복호화한 카운트가 예상되는 값이 아닐 경우, 동기화 오류로 간주하여 단말기에게 재동기화할 것을 요구하도록 하였다. 이를 위해서는 MCC로부터 단말기로 메시지를 송신할 수 있는 회신링크(return link)가 필요한데 COSPAS-SARSAT에는 회신링크를 보유하고 있지 않기 때문에 구체적인 재동기화 방안을 제시하지 못하였다.

2. 갈릴레오 회신링크를 이용한 COSPAS-SARSAT 탐색구조 신호 보안 방식

본 연구에서는 기 제안된 보안 방식에서 단말기와 MCC 간의 동기화를 고려한 COSPAS-SARSAT 탐색구조 신호 보안 방안을 연구하였다. 갈릴레오 시스템의 회신링크 서비스를 이용하여 단말기와 MCC간의 동기화 방식을 설계하였으며, 이를 위해서 기존의 탐색구조 신호 보안 방식을 보완하고 동기화 프로토콜을 설계하였다.

2.1 탐색구조 신호 보안

구조 신호 보안을 위해 고려해야만 하는 제한 사항은 다음과 같다[12].

- 기지국에서 구조 신호를 원활하게 처리하기 위해서 필요한 데이터는 평문으로 전송
- 외부 노출 시 안전성에 영향을 줄 수 있는 위치 정보의 암호화
- 단말기 노출 시 저장된 키 정보의 훼손 가능성 최소화

현재 COSPAS-SARSAT에서 정의하고 있는 여러 사용자 프로토콜 중 국가 사용자 프로토콜은 각 국가별로 임의로 사용할 수 있는 데이터 영역이 가장 넓은 프로토콜이다. 국가 사용자 프로토콜을 사용하는 조난신호는 COSPAS-SARSAT 중계국에서 데이터 해독을 하지 않고 해당 국가로 전달하여 해당 국가의 기관에서 해독할 수 있도록 한다. 따라서 COSPAS-SARSAT 시스템을 이용할 경우 군에서 전송 메시지에 추가적인 보안조치가 가능한 프로토콜이다.

표 8은 COSPAS-SARSAT 장문 메시지의 동기화 비트를 제외한 부분에 대한 국가 사용자 프로토콜 메시지 포맷을 보여준다. 표에서 알 수 있듯이 PDF-1의 46비트와 PDF-2의 26비트가 국가 사용(National Use) 필드로 정의되어 있어, 이 72비트 영역을 자유롭게 정의하여 사용할 수 있다.

표 8. 국가 사용자 프로토콜 메시지 포맷

비트 번호	25				85	86 106	107 132	133 144
필드	61					21	26	12
	First Protected Data Field (PDF-1)					BCH-1	Second Protected Data Field (PDF-2)	BCH-2
서브 필드	1	1	10	3	46	Error Corr. Code for PDF1	National Use	Error Corr. Code for PDF2
	Fmt Flag =1	Prot. Flag =1	Cntry Code	Prot. Code =100	Nat. Use			

PDF-1과 PDF-2에 있는 국가 사용자 필드를 표 9와 같이 설계하였다. 데이터 포맷(Data Format) 필드는 나머지 영역의 포맷을 정의한다. 이 값이 0이면 표 9와 같은 포맷을 가지는 탐색구조 신호를 의미하고, 1이면 다음 절에서 설명할 재동기화를 위한 메시지 신호를 의미한다. 비컨 식별자(Beacon Id)는 단말기를 식별하기 위해 사용한다. 위치 데이터(Position Data)와 위치 보정 데이터(△Position)는 국가 위치 프로토콜과 동일한 포맷을 적용하였다(표 5, 6 참조). 마지막으로 카운트(CNT) 필드는 4장 1절에서와 같이 동기화를 위한 카운트 필드로서 6비트에서 12비트로 길이를 2배로 증가시켰다. 이 중 데이터 포맷 필드와 비컨 식별자를 제외한 53비트(굵은 선으로 표시)를 128비트 AES-CFB 모드로 암호화된다[13].

표 9. 탐색구조 신호를 위한 메시지 포맷

	PDF-1의 국가 사용 필드			PDF-2의 국가 사용 필드	
비트 번호	40	41 58	59 85	107 120	121 132
비트 길이	1	18	27	14	12
필드	Data. Fmt	Beacon Id	Position Data	△Position	CNT
설명	0	단말기 식별자	경위도 좌표 (국가 위치 프로토콜과 동일)	위치 보정 정보 (국가 위치 프로토콜과 동일)	동기화 카운트

AES-CFB 암복호화 처리흐름은 그림 3과 같다. 단말기가 메시지 P를 128비트 키 K로 암호화하기 위해서는 $b(128)$ 비트 IV(Initialization Vector)를 K로 암호화한 다음 그 결과의 좌측 $s(53)$ 비트와 평문 s비트를 배타적 논리합(exclusive-or, ⊕)으로 결합하여 암호문 C를 생성한다. 이 s비트 암호문은 IV에 피드백된다. 즉, IV를 s비트만큼 좌측으로 쉬프트 시키고, 오른쪽 s비트를 암호문으로 채운다. 따라서 암호화를 수행될 때마다 다른 IV를 사용하게 된다.

MCC에서의 복호화 프로세스도 거의 유사하다. IV를 키 K로 암호화한 암호문의 좌측 s비트와 수신한 암호문 C를 논리적 배타합으로 결합하면 평문 P를 얻을 수 있다. 복호화 후, IV는 좌측으로 s비트 쉬프트되고 오른쪽 s비트를 수신한 암호문 C로 채워서 다음 암호문의 복호화에 사용한다[11,12,13,14,15,16].

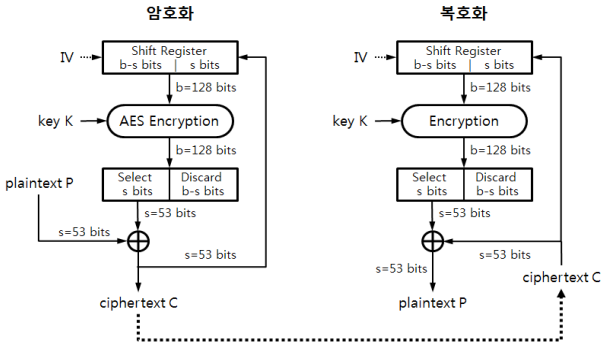

그림 3. 128비트 AES-CFB를 이용한 암복호화

2.2 MCC의 메시지 수신 및 복호화

MCC는 각 단말기에 대하여 공유하는 키와 IV를 이용하여 수신한 메시지의 비컨 식별자로부터 적용할 키와 IV를 결정하여 메시지를 복호화한다.

제안한 방식에서는 CFB 운용모드를 이용한 스트림 암호를 사용하고 있다. 스트림암호에서는 동일한 키를 재사용할 수 없지만, 제안한 방법을 사용할 경우, 전송할 메시지 시퀀스가 달라지면 생성되는 IV값의 시퀀스가 달라지게 된다. 메시지를 보낼 때마다 서로 다른 IV값이 생성되어 다음 메시지 암호화에 사용된다. 따라서 키 자체는 동일하지만, 스트림암호에서의 키 역할을 하는 값은 IV를 키로 암호화한 값이고, 이 값이 매번 달라지므로 키를 재사용하는 문제는 발생하지 않는다. 따라서 단말와 MCC는 최종 암복호화 후 갱신된 IV값(다음 사용할 값)을 저장하고 있어야 한다.

CFB 운용모드를 이용한 스트림암호 방식에서 또 하나 고려해야 할 것은 송수신자간의 동기화이다. 초기에 서로 공유하는 값은 IV와 K이다. 그러나 메시지가 송수신될 때마다 IV값이 달라지게 되는데 메시지의 송신과정에서 메시지가 분실되거나 전송 오류가 발생한다면 MCC는 다음 메시지를 복호화할 수 없게 된다. 이를 위해 12비트 CNT 필드를 할당하여 카운터로 활용한다. CNT의 초기값은 0이며 매 전송마다 1씩 증가하다가 최대값인 $2^{12}-1$(필드의 비트 길이가 12이므로)에 도달하면 다시 0으로 리셋된다.

MCC는 수신된 메시지에서 복호한 카운트값 CNT′이 MCC에 저장된 해당 단말기의 카운트값 CNT보다 1 큰 값인지 확인한다. 그렇지 않으면 동기화에 실패한 것으로 간주하고 단말과 재동기화 프로토콜을 수행하여 IV을 갱신하고 CNT를 초기화한다. 이를 위해 단말과 만약 동기화에 성공하면, MCC는 CNT 값을 1 증가시켜 저장하고 업데이트된 IV를 데이터베이스에 저장한다(그림 4 참조). 이렇게 함으로써 CNT는 암호화된 메시지 필드에 대하여 변조 여부를 판단할 수 있는 무결성도 지원하게 된다.

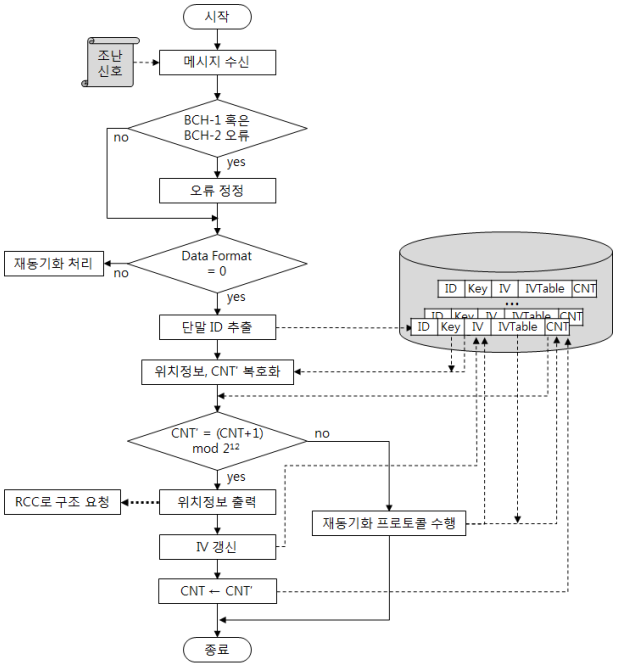

그림 4. MCC의 탐색 구조신호 처리 흐름

단말과 MCC와의 공유키는 재동기화 때 변경되지 않는다. 만일 IV 마저 동일한 값으로 초기화한다면 평문 암호화를 위해 ⊕(배타적 논리합, exclusive or)되는 값이 동일하게 반복되므로 취약점이 될 수 있다. 따라서 단말마다 IV 테이블인 IVTable[]을 보유하고, 재동기화 시 이 테이블에서 갱신할 IV를 선택하도록 하는 것이다. 테이블의 크기는 다음 절에서 설명할 재동기화 프로토콜의 IVX(IV 테이블 색인) 비트길이인 14에 따라 규정된다. MCC에서 단말로부터 메시지를 수신했을 때의 처리 흐름을 그림 4에 도식화하였다.

2.3 COSPAS-SARSAT의 신호 보안 및 Galileo 회신링크를 이용한 동기화 메커니즘

전술한 바와 같이 COSPAS-SARSAT 메시지 구조에서 암호화해야 할 비트길이의 제약으로 인해 AES-CFB 모드를 이용한 스트림 암호방식을 제안하였다. 스트림 암호 방식을 이용하기 위해서는 송수신 사이트의 동기화가 매우 중요하며, 어떠한 이유로 동기화가 이루어지지 않았을 경우에 재동기화하기 위한 방법이 필요하다. 본 장에서는 갈릴레오의 회신링크를 이용한 동기화 방법과 이를 지원하기 위해 보완된 COSPAS-SARSAT 보안 방식을 제안한다.

(1) 키관리 요구사항[11,12]

AES/CFB 모드를 이용한 스트림 암호를 구조신호의 기밀성 유지에 사용하기 위해서 요구되는 키관리 요구사항은 다

음과 같다.

- 단말(비컨)과 MCC간의 암복호화 동기화 기능
- 동기화 오류에 대한 식별 기능
- 동기화 오류 발견 시 재동기화 기능
- 재동기화 기능 수행 시 상호 인증
- 재동기화에 대한 재생 공격 방지

기본적으로 암복호화를 위해 단말과 MCC간의 동기화는 필수적이다. 환경상의 문제나 고의적인 신호 방해로 발생하는 동기화의 오류를 발견할 수 있어야 하며, 오류 발견 즉시 재동기화를 위한 프로토콜을 수행하여 구조 신호를 수신하지 못하거나 지연시키는 상황이 발생하지 않도록 해야 한다. 또한 위장(rogue) 비컨에 의한 재동기화로 구조대를 유인하거나 조난자의 구조를 방해하거나 혹은 자원을 낭비하지 않도록 하고, 위장 MCC로 하여금 암복호화 키나 메시지를 획득하지 못하게 하기 위해서는 재동기화 프로토콜 수행 시 상호 인증할 수 있어야 한다. 마지막으로, 공격자가 이전의 재동기화 프로토콜을 재전송하여 비컨과 MCC간의 통신을 방해하거나 구조를 방해하지 못하도록 재동기화 프로토콜은 재생 공격에 안전해야 한다.

(2) 키관리를 위한 데이터베이스

단말기를 분실하거나 탈취당했을 때, 이 단말로 인하여 다른 단말기의 안전성이 위협받지 않도록 하기 위해서 모든 단말은 서로 다른 암복호화 키와 IV를 사용하도록 한다. COSPAS-SARSAT의 메시지 포맷에는 단말기를 식별할 수 있는 비컨 식별자가 포함되어 있는데 이를 단말 ID로 사용할 수 있다.

단말 T_i의 비컨 B_i는 MCC와 공유한 비밀키 K_i, 최근 사용한 $\mathrm{CNT_i}$, 그리고 랜덤수로 이루어진 IV 테이블 $\mathrm{IVTable_i[]}$와 마지막 암복호화로 생성된 IV값, 즉 다음 암복호화에 사용될 IV값을 보유한다. 또한 각 비컨은 자신을 관리하고 제어하는 MCC들에 대한 목록을 알고 있다.

MCC는 각 비컨에 대하여, 비컨 식별자 B_i, 공유한 비밀키 K_i, 최근 사용한 $\mathrm{CNT_i}$, 그리고 랜덤수로 이루어진 IV 테이블 $\mathrm{IVTable_i[]}$와 마지막으로 생성된 IV값을 저장한다 (4장 2.2절 참조).

따라서 각 단말기는 키 관리를 위하여 표 10과 같은 데이터를 저장하고 있다. 여기서 관리 MCC ID는 이 단말이 등록되어 있고 관리를 담당하고 있는 MCC의 식별자로서, 다음 절의 재동기화 프로토콜에서 사용된다. MCC는 표 11과 같은 데이터를 단말기 수만큼 저장하게 된다. 여기서 IV는 최종 암호화 후 갱신된 IV로서 다음 암복호화에 사용될 IV값이다.

표 10. 단말기에 저장된 데이터와 비트 길이

데이터	단말 ID	관리 MCC ID	Key	IV	IVtable[2^{14}]	CNT
비트 길이	18	10	128	128	128×2^{14}	12

표 11. MCC에 저장된 데이터와 비트 길이

데이터	단말 ID	Key	IV	IVtable[2^{14}]	CNT
비트 길이	18	128	128	128×2^{14}	12

(3) 재동기화 프로토콜

그림 4에서 비컨 B_i으로부터 수신한 신호의 $\mathrm{CNT_i}$ 값이 MCC와 일치하지 않으면 동기화 오류로 판정하고 그림 5와 같이 재동기화 프로토콜을 수행한다.

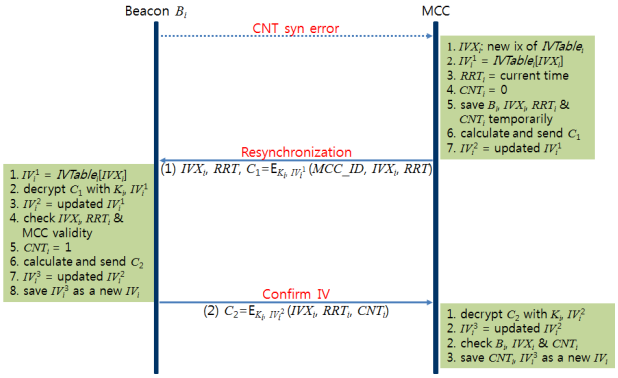

그림 5. 재동기화 프로토콜 흐름도

프로토콜의 세부 수행 내용은 다음과 같다.

[MCC 처리 부분]

① MCC는 B_i가 메시지 암호화에 사용할 새로운 IV를 위해 $\mathrm{IVTable_i[]}$의 새로운 색인인 $\mathrm{IVX_i}$를 랜덤하게 선택한다.

② 재생공격 방지를 위해, 현재의 시각을 재동기화 프로토콜 시작 시각으로서 RRT_i 변수에 저장한다.

③ $\mathrm{CNT_i}$를 0으로 초기화 한다.

④ 프로토콜의 성공적 종료 시까지 B_i, RRT_i 및 $\mathrm{CNT_i}$를 버퍼에 임시 저장한다.

⑤ B_i와 공유한 키 K_i와 새로운 $\mathrm{IV_i^1}$=$\mathrm{IVTable_i[IVX_i]}$를 가지고 MCC의 식별자 MCC_ID와 $\mathrm{IVX_i}$ 및 RRT_i를 암호화한다. 이 암호문을 C_1이라 하자.

$$C_1 = E_{K_i, IV_i^1}(MCC-ID, \mathrm{IVX_i}, RRT_i)$$

⑥ C_1 복호화로 인해 변경된 $\mathrm{IV_i^1}$를 $\mathrm{IV_i^2}$라 하자.

표 12. 재동기화(Resynchronization) 메시지 포맷

비트 번호	68 77	78 91	92 101	102 115	116 142				143 144	145 159
필드	10	14	10	14	27				2	15
	MCC ID	IVTable Index (IVX)	MCC ID	IVTable Index (IVX)	Reset Req. Time (RRT)				Retry	Spare
서브필드					10	5	6	6		
					Year	Month	Date	Hour		

[MCC → B_i: Resynchronization 부분]

① MCC는 B_i에게 $\mathrm{IVX_i}$와 RRT_i, 그리고 암호문 C_1을 전송한다.

[B_i 처리 부분]

① 평문으로 수신한 $\mathrm{IVX_i}$을 가지고 $\mathrm{IV_i^1}$=$\mathrm{IVTable_i}[\mathrm{IVX_i}]$을 계산한다.

② MCC와 공유한 키 K_i와 $\mathrm{IV_i^1}$를 가지고 C_1을 복호화한다.

③ C_1 복호화로 인해 변경된 $\mathrm{IV_i^1}$를 $\mathrm{IV_i^2}$라 하자.

④ 복호화한 $\mathrm{IVX_i}'$이 평문으로 수신한 $\mathrm{IVX_i}$과 같고, 복호화한 $MCC-ID$가 B_i의 관리 MCC 인지, 그리고 RRT_i가 허용된 시간차 범위 내의 현재 시각인지 확인한다. 그렇지 않으면 프로토콜을 종료하고 다시 시작한다.

⑤ $\mathrm{CNT_i}$를 1로 설정한다.

⑥ 갱신된 IV 확인을 위해 K_i와 $\mathrm{IV_i^2}$로 $\mathrm{IVX_i}, RRT, \mathrm{CNT_i}$를 암호화한다. 이 암호문을 C_2라 하자.

$$C_2 = E_{K_i, IV_i^2}(\mathrm{IVX_i}, RRT, \mathrm{CNT_i})$$

⑥ C_2 암호화로 인해 변경된 $\mathrm{IV_i^2}$를 $\mathrm{IV_i^3}$이라 하자.

⑦ $\mathrm{IV_i^3}$를 새로운 $\mathrm{IV_i}$로서 저장한다.

[B_i → MCC: Confirm IV 부분]

① B_i는 성공적 재동기화 확인을 위해 MCC에게 C_2를 전송한다.

[MCC 처리 부분]

① 수신한 메시지 C_2를 복호화하여, 수신한 B_i와 복호화한 $\mathrm{IVX_i}$, RRT_i가 임시 저장된 값과 같고, 복호화한 $\mathrm{CNT_i}$가 저장된 값보다 1 큰 값인지 확인한다. 일치하지 않으면 프로토콜을 재시작한다.

② C_2 암호화로 인해 변경된 $\mathrm{IV_i^2}$를 $\mathrm{IV_i^3}$이라 하자.

③ 재동기화가 성공적으로 이루어졌으므로, $\mathrm{CNT_i}$와 $\mathrm{IV_i^3}$를 B_i의 데이터로 저장한다.

(4) 메시지 포맷

① Resynchronization

MCC에서 B_i로부터 수신한 구조 메시지의 $\mathrm{CNT_i}$ 오류로 인하여 재동기화를 요구하는 메시지는 갈릴레오 RLM의 COMMAND 서비스를(메시지 코드 2) 이용한다(표 7 참조). 메시지 포맷은 표 12와 같이 95비트의 데이터 필드를 가진다. 데이터 필드 중 첫 3비트는 CMD 필드로서 MCC가 전송하고자 하는 명령을 의미한다. CMD 코드는 표 13과 같으며 아직 정의되어 있지 않은 101(2) = 5(10)에 'Resynchronization' 커맨드를 할당하여 사용하도록 제안한다.

표 12의 68-159비트의 데이터 필드에 대한 상세한 메시지 포맷은 표 14와 같다. MCC-ID는 10비트를 가진다. IVTable 색인은 14비트이며, 결과적으로 IVTable은 최대 2^{14}=16384개의 엔트리를 가질 수 있다. 다음 53비트는 MCC-ID, IVX, RRT 및 Retry 필드의 암호화된 값이다.

RRT는 재동기화 프로토콜을 시작하는 27비트 시간 정보로서, 세부 필드는 모두 무부호 정수이며 표 15와 같이 정의된다. Year 필드는 재동기화를 수행하는 실제 연도에서 2015를 뺀 값이다. 즉, 2030년은 $2030_{(10)}-2015_{(10)} = 15_{(10)} = 0001111_{(2)}$로 표현된다. Month, Date, Hour는 각각 재동기화 시작 시각의 월, 일, 시를 나타낸다. Minutes는 분 정보를 나타내는데, 정밀도가 2이다. 즉, 이 필드값이 $11001_{(2)}=25_{(10)}$이면 50분을 나타낸다. 분 정보는 실제 분값에 가까운 값을 사용한다. 따라서 오차는 1분 이내이다. Year 필드가 7비트로 제한되기 때문에 2142년 12월 31일 23시 59분 이전까지 사용할 수 있다.

표 13. 갈릴레오 장문 회신 메시지의 커맨드 메시지 구조

비트 번호	1 60	61 64	65 67	68 159	160
비트 길이	60	4	3	92	1
필드	Beacon ID	Message Code=2	CMD	Data	Parity

표 14. 커맨드 코드 할당

CMD 코드	커맨드 의미	비고
0	Beacon Burst Change	
1	Remote Beacon De-activation	
2	Remote Beacon Activation	
3	Beacon Off Confirmation	
4	Test Burst Request	
5	TBD → Resynchronization	본 연구에서 할당
6	TBD	
7	TBD	

Retry 필드는 Resynchronization 메시지의 재전송에 사용된다. RRT가 2분의 정밀도를 가지기 때문에, 재동기화 프로토콜 수행 과정에서 비정상적으로 종료되어, 동일한 RRT를 가지고 재동기화를 재시작할 경우를 처리하기 위한 것이다. Resynchronization 메시지를 수신한 비컨은 Confirm IV 메시지를 MCC에게 송신하여 서로 동일한 IV로 재동기화 되었음을 확인하는데, 만약 이 과정이 성공하지 못하거나, 일정시간 동안 MCC가 Confirm IV를 수신하지 못했을 경우에는 Resynchronization 메시지를 재전송한다. 2비트 Retry 필드는 0에서 시작하여 재동기화 프로토콜의 실패로 인해 재시작할 때마다 (Retry+1) mod 4로 변경된다. 이를 통해 비컨은 수신한 Resynchronization 메시지가 새로운 재동기화 프로토콜의 시작인지 재전송하는 것인지를 구분할 수 있다. 단, 재시작이라고 해도 RRT가 바뀔 경우에는 IVX를 새로 선정하고 Retry 값은 0으로 리셋된다. 이는 비컨이 동일한 재동기화 메시지를 여러 개 수신했을 때 처리할 수 있도록 하기 위한 것이기 때문에 Confirm IV 메시지에서는 이 필드가 포함되지 않는다. 따라서 재시작하는 경우를 제외하고는 2분 이내에 2개 이상의 새로운 재동기화 프로토콜은 수행할 수 없으며, 동일한 RRT를 가지고 재동기화 프로토콜을 최대 4번까지 수행할 수 있다.

표 15. RRT 필드 정보

비트 길이	필드	설 명
7	Year	0-127의 값을 가진다. 연도-2015. 정밀도는 1년
4	Month	1-12의 값을 가진다. 정밀도는 1개월
5	Date	1-31의 값을 가진다. 정밀도는 1일
5	Hour	0-23의 값을 가진다. 정밀도는 1시간
6	Minute	0-29의 값을 가진다. 정밀도는 2분

② Confirm IV

이 메시지는 구조 위치 신호 메시지와 마찬가지로 표 8의 국가 사용자 프로토콜을 이용한다. 국가 사용 필드에 대한 포맷은 표 16과 같다. 표 9의 탐색구조 신호와 마찬가지로 1비트 데이터 포맷 필드는 나머지 필드를 정의하는 필드로서, 1이면 Confirm IV 메시지임을 나타낸다. 다음 18비트는 비컨 식별자이고, 그 다음 27비트 RRT는 MMC로터 수신한 RRT와 동일한 포맷과 값을 가진다. PDF-2의 14비트 IVX도 MMC로부터 수신한 값이고, 12비트 CNT는 재동기화된 이후의 카운터 값으로서 1이다. MMC, IVX 및 CNT 필드는 암호화되는 필드로서 53비트 길이를 갖는다.

표 16. Confirm IV 메시지 포맷

	PDF-1의 국가 사용 필드			PDF-2의 국가 사용 필드	
비트 번호	40	41 58	59 85	107 120	121 132
비트 길이	1	18	27	14	12
필드	Data Format =1	Beacon Id	Resynch. Request Time (RRT)	IVTable Index (IVX)	CNT

V. 결론 및 토의사항

본 논문에서는 개인, 선박 혹은 비행기 조난 시 COSPAS-SARSAT을 이용한 탐색구조 신호를 분석하고 보안 방안을 제시하였다. 가장 중요한 위치 정보의 기밀성을 유지하기 위해서는 위치 정보에 AES-CFB 운용모드를 적용하여 암호화하도록 하였고, 이를 위해 COSPAS-SARSAT 프로토콜 중 국가 사용자 프로토콜을 이용하여 메시지 형식을 설계하였다. AES-CFB 모드는 스트림 방식으로 암호화를 수행하며 송수신자간의 동기화가 필수적이기 때문에, 동기화에 실패했을 경우에는 재동기화가 필요하게 된다. 또한 재동기화는 MCC가 단말에 지시함으로써 이루어져야 하므로 회신링크의 구현이 필수적이다. 따라서 본 논문에서는 현재 COSPAS-SARSAT과의 회신링크 연계가 논의되고 있는 갈릴레오 시스템의 회신링크를 이용하여 재동기화 프로토콜 및 그에 필요한 메시지 포맷을 설계하였다.

제안한 방식은 이미 규격이 정의되어 있는 기존의 시스템을 활용해야 하는 제한 사항을 내포하고 있다. 즉, 재생공격을 방지하기 위한 시각 정보 RRT의 연(Year) 필드가 7비트로 한정되기 때문에 재동기화 프로토콜 사용연한이 2142년 12월 31일 23시 59분 이전까지로 제한된다. 또한 RRT의 정밀도가 2분이기 때문에 실제 시각과의 오차는 최대 1분이고 재동기화 프로토콜은 최대 2분에 1번 수행할 수 있으며, 재동기화 프로토콜을 2분 이내 새로 시작할 수 없다. 마지막으로 IVX 필드의 길이가 14비트이기 때문에 단말의 IV 테이블의 엔트리 수는 최대 2^{14} = 16,384개로 제한된다.

본 논문에서 제안된 방식은 MCC가 탐색구조 신호를 수신해야만 재동기화를 수행하도록 되어 있다. 따라서 위급 상황 시 빠른 구조 작업이 수행되어야 함을 고려한다면, 실제 동기화 오류 확률을 분석하여 정기적인 재동기화를 수행할 필요가 있는지에 대한 추후 연구가 필요할 것으로 보인다.

참 고 문 헌

[1] COSPAS-SARSAT, https://www.COSPAS-SARSAT.int/en/system-overview/COSPAS-SARSAT-system

[2] 위성항법중앙사무소, GALILEO 개요, "http://www.ndgps.go.kr/html/kr/dgpsys/dgpsys_0205.html.
[3] COSPAS-SARSAT, Specification for COSPAS-SARSAT 406MHz Distress Beacon C/S T.001, OCT. 2012.
[4] Innovative Project, http://www.indracompany.com/en/sostenibilidad-e-innovacion/proyectos-innovacion/gsarsed-galileo-sar-service-early-demonstration-139.
[5] ESA, http://www.esa.int/spaceinimages/Images/2012/03/LEOSAR_and_GEOSAR_satellites.
[6] ILRS, http://ilrs.gsfc.nasa.gov/missions/satellite_missions/current_missions/ga01_general.html.
[7] 김재현, 이상욱, 백유진, 조태남, 안우근, "COSPAS-SARSAT MEOSAR 회신링크 서비스를 이용한 탐색구조 신호보안", ISGNSS 2014 in conjunction with KGS Conference, pp.702-705, 2014.
[8] JC-26/Inf.27, "SAR/GALILEO RETURN LINK SYSTEM MESSAGE SPECIFICATION," May 2012.
[9] JC-26/Inf.27: RETURN LINK SERVICE OF TYPE-2, MAY 2013.
[10] JC-26, "RLS Type-1 Message Definition and Standardization," May 2012.
[11] 조태남, 백유진, 군 탐색구조 시스템 상용망 연동 비화 기법 연구, 한국전자통신연구원 연구용역 보고서(EA-2013-2143), 2013.
[12] 백유진, 조태남, 김재현, 이상욱, 안우근, "COSPAS-SARSAT을 이용한 탐색구조 신호 보안", 제어, 로봇, 시스템 학회 논문지 제20권 제 2호, pp.157-161, 2014.
[13] FIPS-197, "Advanced encryption standard (AES)," 2001.
[14] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, Handbook of Applied Cryptography, 5th Ed.,CRCPress,1996.
[15] IEEE, "Standard for cryptographic protection of data on block-oriented storage services," IEEE P1619/D16, 2007.
[16] W. Stallings, Cryptography and Network Security, 5th Ed., Pearson, 2011.

저자

조 태 남(Taenam Cho)

・1986년 2월 : 이화여자대학교 전자계산학과 (학사)
・1988년 2월 : 이화여자대학교 전자계산학과 (석사)
・2004년 2월 : 이화여자대학교 컴퓨터학과 (박사)
・1988년 ~ 1996년 : 한국전자통신연구원 선임연구원
・2005년 ~ 현재 우석대학교 정보보안학과 부교수
<관심분야> : 암호프로토콜, 네트워크 보안, 안드로이드 보안

백 유 진(Yoojin Baek) **교신저자**

・1997년 2월 : 서울대학교 수학과(학사)
・1999년 2월 : 서울대학교 수학과(석사)
・2003년 2월 : 서울대학교 수리과학부 (박사)
・2003년 ~ 2003년 : KAIST 박사후 연구원
・2003년 ~ 2013년 : 삼성전자 책임 연구원
・2013년 ~ 현재 : 우석대학교 정보보안학과 부교수
<관심분야> : 부채널 공격, 정보 보안

김 재 현(Jaehyun Kim)

・2005년 2월 : 한양대학교 전자전기컴퓨터공학부 (학사)
・2007년 2월 : 한양대학교 전자통신컴퓨터공학과 (석사)
・2007년 ~ 현재 한국전자통신연구원 위성항법연구실 선임연구원
<관심분야> : 위성항법,신호처리,무선통신,탐색구조시스템

이 상 욱(Sanguk Lee) **정회원**

・1988년 2월 : 연세대학교 천문기상학과 (학사)
・1991년 2월 : Auburn 대학교 항공우주공학과 (석사)
・1994년 2월 : Auburn 대학교 항공우주공학과 (박사)
・1993년 ~ 현재 한국전자통신연구원 위성항법연구실 책임연구원
<관심분야> : 위성시스템 및 제어, 위성항법, 탐색구조시스템

안 우 근(and Woo-Geun Ahn)

・2001년 2월 : 고려대학교 전기전자전파공학부 (학사)
・2003년 2월 : KAIST 전기 및 전자공학과 (석사)
・2010년 2월 : KAIST 전기 및 전자공학과 (박사)
・2011년 ~ 현재 국방과학연구소 항법기술부 선임연구원
<관심분야> : 위성항법, 신호처리, 무선통신