Journal of Institute of Control, Robotics and Systems (2014) 20(2):157-162
http://dx.doi.org/10.5302/J.ICROS.2014.13.9009 ISSN:1976-5622 eISSN:2233-4335

COSPAS-SARSAT 을 이용한 탐색구조 신호 보안

Secured Search and Rescue Signal using COSPAS-SARSAT

백 유 진, 조 태 남*, 김 재 현, 이 상 욱, 안 우 근
(Yoojin Baek[1], Taenam Cho[1,*], Jaehyun Kim[2], Sanguk Lee[2], and Woo-Geun Ahn[3])
[1]Dept. of Information Security, Woosuk University
[2]Satellite & Wireless Convergence Research Department, Electronic Telecommunications Research Institute
[3]The 3rd R&D Institute, Agency for Defense Development

Abstract: The international COSPAS-SARSAT program is a satellite-based search and rescue distress alert detection and information distribution system and best known as the system that detects and locates emergency beacons activated by aircraft, ships and so on. However, the current message format of the system is not encrypted so that, if the rescue signal can be intercepted by the unintended receivers, the subsequent rescue activities can be handled in a hostile environment. So, this article concerns how to deal with the rescue signals in a secure way and proposes some adequate encryption methods and the corresponding key management.

Keywords: COSPAS-SARSAT, search and rescue signal, satellite, encryption, authentication

I. 서론

COSPAS-SARSAT (Cosmicheskaya Sistema Poiska Avariynyh Sudov[translated into Space System for the Search of Vessels in Distress] - Search And Rescue Satellite-Aided Tracking) 프로그램은 위성 기반의 조난 검색 및 구조 시스템으로서 1979년에 캐나다, 프랑스, 미국 및 옛 소련에 의해 처음 설립되었고 2011년 현재 대한민국을 포함한 26개 국가가 참여하고 있으며 항공기나 선박 등에 의해 활성화된 탐색구조(SAR: search and rescue) 신호를 탐지하고 그 위치를 특정할 수 있는 시스템으로 잘 알려져 있다. 현재 운용되는 있는 COSPAS-SARSAT 위성을 이용한 단말기는 주로 저궤도 탐색구조(LEOSAR) 시스템에서 도플러 신호처리를 이용하여 조난자의 위치를 추적하고 정지궤도탐색구조(GEOSAR) 시스템에서 GPS칩을 이용하여 조난자의 위치를 추적하여 해당 선박이나 항공기, 조난자를 식별하는 형태로 운용되고 있다[1].

비행기, 선박, 개인은 각각 ELT (Emergency Locator Transmitters), EPIRB (Emergency Position-Indicating Radio Beacon), PLB (Personal Locator Beacons)라고 불리는 탐색구조 단말기를 소유하고, 유사시에 COSPAS-SARSAT으로 조난자의 위치정보가 포함된 구조신호를 보낸다. COSPAS-SARSAT은 수신한 이 신호를 지상으로 중계한다. 지역수신지구국 LUT (Local User Terminal)는 위성으로부터 신호를 받아 임무통제본부 MCC (Mission Control Center)로 전송한다. MCC에서는 구조조정본부 RCC (Rescue Coordination Center)로 구조를 요청하고

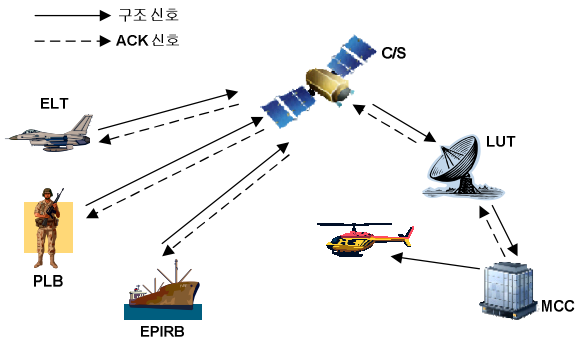


그림 1. 위성을 이용한 탐색구조.
Fig. 1. Search and rescue using satellite.

단말에게 신호를 수신하였음을 알리는 ACK 메시지를 송신한다(그림 1 참조).

이를 위해서 사용되는 메시지 포맷은 COSPAS-SARSAT 관리문서 형식으로 사무국에서 관리되고 있으나 이러한 메시지 포맷은 그 특성상 어떠한 보안 서비스가 제공되지 않고 있기 때문에, 만약 원치 않는 상대방에 의해서 탐색구조 신호가 가로채질 경우 그 후속 구조 활동에서의 안전성을 매우 취약하게 만든다. 가령 군 장병이 조난을 당하는 경우 현재의 메시지 포맷을 이용하여 구조 신호를 보내게 되면 해당 장병의 위치 정보가 고스란히 적에게 노출될 우려가 있다. 적군이 먼저 이러한 신호를 먼저 탐지했을 경우 해당 장병의 안전성 및 그가 가지고 있을 수 있는 정보의 안전성을 심각하게 훼손할 우려가 있다.

본 논문에서는 COSPAS-SARSAT 위성을 이용한 탐색 구조 단말기의 구조 신호에 사용되는 메시지 포맷을 분석하고 위치 정보와 같은 민감한 정보에 대한 암호화 방법을 제안하며, 그리고 이러한 암호화 서비스 제공 시 사용될 암호키의 안전한 저장 및 처리 방식 등에 대한 새로운 방법을 제안한다.

* Corresponding Author
Manuscript received November 20, 2013 / revised December 20, 2013 / accepted December 31, 2013
백유진, 조태남: 우석대학교 정보보안학과
(yjbaek@ws.ac.kr/tncho@ws.ac.kr)
김재현, 이상욱: 한국전자통신연구원 위성무선융합연구부
(longinus@etri.re.kr/slee@etri.re.kr)
안우근: 국방과학연구소 제3기술연구본부(wgahn@add.re.kr)
※ 본 연구는 방위사업청과 국방과학연구소가 지원하는 국방위성항법 특화연구센터 사업의 일환으로 수행되었음.

	Bit Synchronization	Frame Synchronization	First Protected Data Field (PDF-1)				BCH-1	Non-Protected Data Field
Unmodulated Carrier (160 ms)	Bit Synchronization Pattern	Frame Synchronization Pattern	Format Flag	Protocol Flag	Country Code	Identification or Identification plus Position	21-Bit BCH Code	Emergency Code/ National Use or Supplement. Data
Bit No.	1-15	16-24	25	26	27-36	37-85	86-106	107-112
	15 bits	9 bits	1 bit	1 bit	10 bits	49 bits	21 bits	6 bits

그림 2. COSPAS-SARSAT 탐색구조 신호의 단문 메시지 포맷[1].
Fig. 2. Short Message Format of COSPAS-SARSAT Search and Rescue Signal [1].

	Bit Synchronization	Frame Synchronization	First Protected Data Field (PDF-1)				BCH-1	Second Protected Data Field (PDF-2)	BCH-2
Unmodulated Carrier (160 ms)	Bit Synchronization Pattern	Frame Synchronization Pattern	Format Flag	Protocol Flag	Country Code	Identification or Identification plus Position	21-Bit BCH Code	Supplementary and Position or National Use Data	12-Bit BCH Code
Bit No.	1-15	16-24	25	26	27-36	37-85	86-106	107-132	133-144
	15 bits	9 bits	1 bit	1 bit	10 bits	49 bits	21 bits	26 bits	12 bits

그림 3. COSPAS-SARSAT 탐색구조 신호 장문 메시지 포맷[1].
Fig. 3. Long Message Format of COSPAS-SARSAT Search and Rescue Signal [1].

Format Flag (bit 25) → Protocol Flag (bit 26) ↓	0 (short)	1 (long)
0 (protocol code: bits 37-40)	Not Used	Standard Location Protocols National Location Protocols RLS Location Protocols
1 (protocol code: bits 37-39)	User Protocols	User Protocols User-Location Protocols

그림 4. Format Flag와 Protocol Flag의 결합 방식[1].
Fig. 4. Format Flag and Protocol Flag Combinations [1].

II. COSPAS-SARSAT 탐색구조신호 메시지 포맷 분석

COSPAS-SARSAT 탐색구조신호에 사용되는 메시지 포맷은 COSPAS-SARSAT 관리문서 형식으로 사무국에서 관리되고 있으며 메시지 데이터포맷은 장문의 경우 송신 메시지 144 bit의 520 ms ± 1 percent, 400bps ±1 percent를 만족하여야 하고, 단문의 경우 송신 메시지 112 bit의 440 ms ± 1 percent, 400bps ±1 percent 를 만족하여야 한다. COSPAS-SARSAT 메시지는 단문과 장문의 2가지 포맷을 지원한다. 단문 메시지 포맷은 112비트 길이로 구성되며, 장문 메시지 포맷은 단문 메시지에 포함된 위치 정보의 정확도를 높이기 위한 정보가 추가된 포맷으로서 144비트의 길이를 가진다. 그림 2와 그림 3은 이러한 구조신호의 단문 및 장문 메시지 포맷을 나타내며 데이터 포맷 구성표에서 무변조 데이터가 160ms 동안 송신된 뒤부터 장문과 단문에 따라 나머지 360ms 및 280ms 동안에 해당 데이터가 송신된다.

단문 메시지 포맷의 1-24 비트는 비트동기와 프레임 동기 비트 정보로서 데이터를 수신하기 위한 데이터이고, 다음 25-85 비트의 PDF1 영역은 전송하고자 하는 조난자 정보 등을 담고 있다. 이는 초창기 단문형태로 개발되었던 포맷이다. 하지만, GPS 정보를 같이 송신할 수 있는 단말기가 사용됨에 따라 위치 정보의 정확도를 높이기 위하여 두 번째 데이터 영역 PDF-2(107-132 비트)를 추가한 형태가 그림 2의 장문 메시지가 된다. 단/장문 메시지의 86-106 비트의 BCH-1과 장문 메시지의 133-144 비트의 BCH-2는 구조신호의 전송 중에 발생할 수 있는 통신 오류를 탐지/정정할 수 있는 오류정정 부호에 사용되며 COSPAS-SARSAT 위성 탐색구조신호의 경우 BCH 코드가 사용된다. BCH-1은 PDF-1에 대한 코드이며 BCH-2는 PDF-2에 대한 코드이다.

메시지가 단문인지 장문인지는 25번째 비트에 따라 결정된다. 이 비트는 조난신호의 포맷을 나타내는 "F" 형식 플래그로서 "0"은 단문을 "1"은 장문을 나타낸다. 26번째 비트는 탐색구조에서 사용 가능한 부호화된 데이터의 구조를 나타내는 프로토콜들 중 사용된 특정한 프로토콜을 나타내는 "P" 형식 플래그로서 "0"은 표준 위치 프로토콜이나 국가 위치 프로토콜을 "1"은 사용자 프로토콜이나 사용자 위치 프로토콜을 나타낸다. 이러한 프로토콜 정보는 이후 37번째부터 85번째 비트까지의 Identification or Identification plus Position 필드 중 첫 3비트 또는 4비트 정보를 결정하게 되며 자세한 필드 설정 방식은 그림 4에 좀 더 자세히 나타나 있다.

27번째 비트에서 36번째 비트까지 총 10비트는 ITU에서 관리하는 MID (Maritime Identification Digit) 국가코드를 나타내며 한국의 경우 440(10)과 441(10) MID 코드를 가진다. 따라서 국가코드는 "440(10) = 0110111000(2)" 혹은 "441(10) = 0110111001(2)"로 나타낼 수 있다.

37-85 비트의 Identification or Identification plus Position 필드는 실제 데이터가 들어가는 부분으로 그 중 처음 3비트나 4비트는 위에서 설명하였듯이 다양한 프로토콜들 중 현재 사용되는 프로토콜을 나타내고(그림 4 참조), 그 외의 데이터에

	Bit Synchronization	Frame Synchronization	PDF-1					BCH-1	Non-Protected Data Field
Unmodulated Carrier (160 ms)	Bit Synchronization Pattern	Frame Synchronization Pattern	Format Flag	Protocol Flag	Country Code	Protocol Code	National Use	21-Bit BCH Code	Emergency Code/ National Use or Supplement. Data
Bit No.	1-15	16-24	25	26	27-36	37-39	40-85	86-106	107-112
Value	···	...	F	1	...	1 0 0	...		...

그림 5. 국가 사용자 프로토콜의 메시지 포맷[1].
Fig. 5. Message Format of National User Protocol [1].

		PDF-1						PDF-2			
	Bit & Pattern Synchronization	Format & Protocol Flag	Country Code	Protocol Code	National ID Number	Location Info	BCH-1	Suppl. Data	Location Info	National Use	BCH-2
Bit No	1-24	25-26	27-36	37-40	41-58	59-85	86-106	107-112	113-126	127-132	133-144

그림 6. 국가 위치 프로토콜의 메시지 포맷[1].
Fig. 6. Message Format of National Location Protocol [1].

는 해상이동업무용 식별부호 (MMSI) 및 비콘(beacon) 번호를 할당해 동일한 선박에 여러 개의 비콘을 탑재할 때 이를 구별하기 위해 사용된다. 단문 메시지의 107-112 비트와 장문 메시지의 107-132 비트는 응급 상황이나 국가 사용을 위한 코드 또는 여분의 데이터용으로 할당되었다.

III. COSPAS-SARSAT 구조 신호에 대한 보안 방식 제안

현재 COSPAS-SARSAT에서 정의하고 있는 여러 사용자 프로토콜 중 국가 사용자 프로토콜은 각 국가별로 임의로 사용할 수 있는 데이터 영역을 둔 프로토콜로서, 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 전송 메시지에 추가적인 보안조치가 가능한 프로토콜이다. 이 때 메시지 형태에 따라 단문일 경우에는 국가 사용자 프로토콜, 장문일 경우에는 국가 위치 프로토콜로 분류할 수 있으며, 두 프로토콜의 차이는 장문에 따른 추가적인 데이터 영역의 존재유무이다. 각 메시지의 포맷은 그림 5 및 그림 6과 같다.

다음 절에는 이 메시지 포맷에 적합한 대한 암호화 방식을 제안하고자 한다. 이를 위해 먼저 보안을 제공하기 위해 고려해야 할 사항을 분석한다.

1. 보안 고려 사항

탐색구조 신호에 대한 최소 보안요구사항은 다음과 같다.

① 외부 노출 시, 안전성에 영향을 줄 수 있는 위치 정보의 기밀성 제공
② 단말기 분실/도난 시 다른 단말기로의 영향 최소화
③ 공격자의 메시지 위변조 공격에 대응
④ 단말기의 장기 사용에 대한 보안 위험성 완화

이러한 보안 요구사항을 해결하기 위해 고려해야 하는 제한사항은 다음과 같다.

① 기존 메시지 포맷 준수
② 위성 및 MCC가 기존 메시지와 제안 메시지를 구분 처리 가능
③ 보안기술 적용과 무관하게 전송 오류 정정 가능

2. 메시지 보안

앞에서 기술한 보안요구사항 및 제한사항을 반영한 각 필드에 대한 처리 방식은 다음과 같다.

① Bit & Pattern Synchronization, Format & Protocol Flag, Country Code, Protocol Code, National ID Number 는 평문으로 전송 (제한사항 ②)
② 위치 정보와 장문 메시지 포맷의 127-132비트의 National Use 필드를 암호화(보안요구사항 ①)
③ 암호문의 길이는 기존 필드와 동일하게 유지(제한사항 ①)
④ 암호화 적용 후 PDF1 영역에 대한 BCH 코드 생성 및 장문 메시지 포맷의 경우 PDF2 영역에 대한 BCH 코드 생성(제한사항 ③)
⑤ 각 단말은 서로 다른 암복호화 키를 사용(보안요구사항 ②)
⑥ 메시지 위변조를 확인할 수 있는 정보를 메시지에 포함 (보안요구사항 ③)
⑦ 암복호화키는 지속적으로 변경(보안요구사항 ④)

처리방식 ①-④은 본 절의 “메시지 암호화”를 통해 기술하고, 처리방식 ⑤-⑦는 다음절 “키관리 구조”를 통해 기술한다.

각 메시지 포맷에 상기 처리 방식을 적용하였을 경우 암호화되는 데이터 필드를 그림 7과 그림 8에 점선으로 표시하였다.

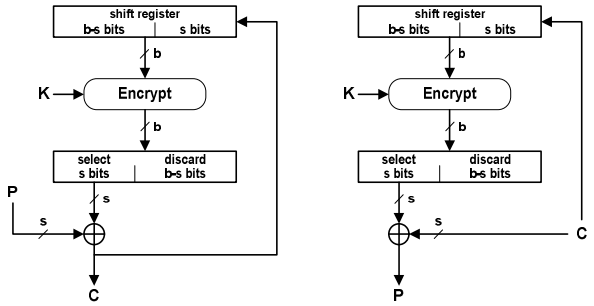
따라서 암호화되어 보호될 위치정보 필드는 단문 메시지 포맷의 경우 27비트의 크기를 가지며 장문 메시지 포맷의 경우 47 비트 크기를 가지게 된다. 따라서 64비트 블록 크기를 가지는 DES나 128비트 블록 크기를 가지는 AES [5] 등의 블록 암호는 적용하기 어려우며 스트림 암호 방식을 적용하는 것이 바람직하다. 본 논문에서는 블록 운용모드 중 CFB (Cipher FeedBack) 모드를 [4] 활용한다. 암호화 알고리즘으로는 128비트 AES를 이용한다. 그림 9는 암복호화 하고자 하는 메시지의 길이가 암복호 알고리즘의 블록 크기인 b비트 이하일 경우에 CFB 운용모드로 암복호화 할 경우를 보여준다. 이 경우 각 메시지 포맷에 대한 위치 정보를 암호화하기 위

	Bit Synchronization	Frame Synchronization	PDF-1					BCH-1	Non-Protected Data Field
Unmodulated Carrier (160 ms)	Bit Synchronization Pattern	Frame Synchronization Pattern	Format Flag	Protocol Flag	Country Code	Protocol Code	National Use ID	21-Bit BCH Code	Emergency Code/ National Use or Supplement. Data
Bit No.	1-15	16-24	25	26	27-36	37-39	40-85	86-106	107-112
Value	···	...	F	1	...	1 0 0	...		...

그림 7. 단문 메시지의 암호화가 적용될 데이터 필드.
Fig. 7. Data fields to be encrypted in Short Message Format.

		PDF-1						PDF-2			
	Bit & Pattern Synchronization	Format & Protocol Flag	Country Code	Protocol Code	National ID Number	Location Info	BCH-1	Suppl. Data	Location Info	National Use	BCH-2
Bit No	1-24	25-26	27-36	37-40	41-58	59-85	86-106	107-112	113-126	127-132	133-144

그림 8. 장문 메시지의 암호화가 적용될 데이터 필드.
Fig. 8. Data fields to be encrypted in Long Message Format.



(a) Encryption. (b) Decryption.

그림 9. CFB 운용 모드.
Fig. 9. CFB Operational Mode.

해서는 암호화 비트 길이인 s는 메시지 포맷이 단문 혹은 장문인지에 따라 각각 27 비트 혹은 47 비트가 되며, b는 AES의 블록 크기인 128비트가 된다.

단말기가 메시지 P를 키 K로 암호화하기 위해서는 IV (Initialization Vector)를 K로 암호화한 다음 그 결과의 왼쪽 s 비트와 평문 s 비트를 배타적 논리합(exclusive-or, ⊕)으로 결합하여 암호문 C를 생성한다. 이 s 비트 암호문은 IV에 피드백된다. 즉, IV를 s비트만큼 왼쪽으로 쉬프트 시키고, 오른쪽 s비트를 C로 채운다. 따라서 암호화를 수행될 때마다 다른 IV를 사용하게 된다. MCC에서의 복호화 프로세스도 거의 유사하다. IV를 키 K로 암호화한 암호문의 왼쪽 s 비트와 수신한 암호문 C를 논리적 배타합으로 결합하면 평문 P를 얻을 수 있다. 복호화 후, 역시 IV는 왼쪽으로 s비트 쉬프트되고 오른쪽 s비트를 수신한 암호문 C로 채워서 다음 암호문의 복호화에 사용한다. OFB (Output FeedBack) 모드는 CFB와 유사하지만 IV로 피드백되는 값이 다르다. OFB에서는 메시지의 암호문이 아니라 IV를 암호화한 값의 왼쪽 s비트가 IV로 피드백된다. OFB를 사용할 경우 IV의 암호화한 결과가 주기적으로 반복된다는 단점을 가지기 때문에 CFB가 더 적합하다. 스트림 암호를 사용할 경우 송수신자간의 키에 대한 동기화가 필수적이다. 이에 대해서는 다음 절인 "키관리 구조"에서 다룬다.

표 1. 단말기에 저장된 데이터.
Table 1. Data Stored in User Terminal.

데이터	단말 ID	Key	IV	CNT
비트길이	18	128	128	6

3. 키관리 구조

암호키 저장 및 관리는 제안된 암호화 방식에서 또 다른 보안 사항 중 하나이다. 가령, 상기 알고리즘을 구현한 단말기가 모두 동일한 키를 사용할 경우 한 단말기의 분실은 전체 시스템의 안전성에 커다란 위협이 된다. 즉, 공격자가 분실한 단말기를 습득하거나 탈취하여 키를 얻게 되면, 다른 단말기로부터의 탐색구조 신호를 복호화 함으로써 조난자의 위치를 파악할 수 있게 된다. 가장 간단한 방법은 각 단말기마다 다른 키를 사용하도록 하는 것이다. 이것은 보안요구사항 ②를 지원한다.

COSPAS-SARSAT의 단문 및 장문 메시지 포맷에는 단말기를 식별할 수 있는 비콘 번호가 포함되어 있는데 이를 단말 ID로 사용할 수 있다(II장 참조). 따라서 각 단말기가 서로 다른 키를 사용하도록 하고, 그 키를 MCC와 공유하도록 한다. MCC에서는 수신한 메시지의 단말 ID로부터 복호화에 사용할 키를 결정할 수 있다. 따라서 각 단말기는 키 관리를 위하여 표 1과 같은 데이터를 저장하고 있으며, MCC는 표 1과 같은 데이터를 단말기 수만큼 저장하고 있다.

단말 ID는 단문 및 장문 메시지에 포함된 단말 ID와 동일한 값이다. Key는 AES에 사용될 키이고, IV는 CFB 운용모드에서 사용된 최종값이다.

제안한 방식에서는 CFB 운용모드를 이용한 스트림 암호를 사용하고 있다. 스트림 암호에서는 동일한 키를 재사용해서는 안된다. 제안한 방법을 사용할 경우, 전송할 메시지 시퀀스가 달라지면 생성되는 IV값의 시퀀스가 달라지게 된다. 또한 IV는 비밀값일 필요가 없으며, 모든 단말기가 초기 IV 값을 동일하게 가지더라도 메시지를 보낼 때마다 서로 다른 IV값이 생성되어 다음 메시지 암호화에 사용된다. 따라서 키 자체는 동일하지만, 스트림 암호에서의 키 역할을 하는 값은 IV를 키로 암호화한 값이고, 이 값이 매번 달라지므로 키를

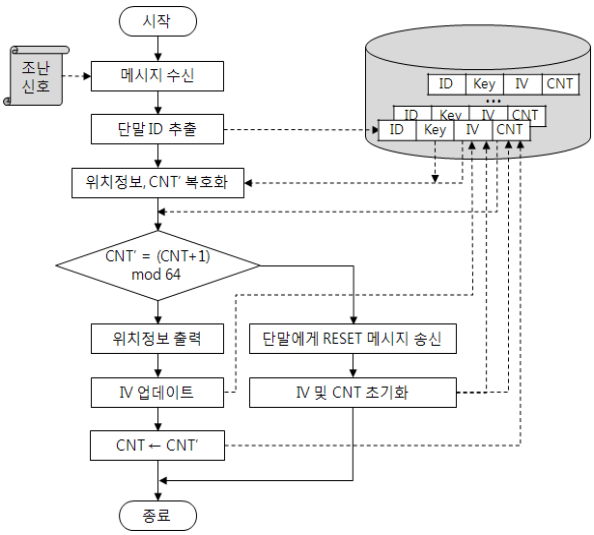


그림 10. MCC의 메시지 처리 흐름도.
Fig. 10. Message Processing Flow of MCC.

재사용하는 문제는 발생하지 않는다. 따라서 단말은 마지막 IV 값을 저장하고 있어야 하며, MCC는 단말마다 마지막 사용한 IV값을 표 1과 같이 저장하고 있어야 한다. 이로써 보안요구사항 ④를 지원한다.

CFB 운용모드를 이용한 스트림 암호 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 복호화 할 수 없게 된다. 장문 메시지 포맷을 이용할 경우, National Use 필드를 이용하여 이를 방지할 수 있다.

이 필드는 127-132 비트로서 6비트 길이를 가지는데 이 필드를 카운터로 활용한다. 이를 CNT라 하자. CNT의 초기값은 0이며 매 전송마다 1씩 증가하다가 최대값인 63에 도달하면 다시 0으로 리셋된다.

MCC는 수신된 메시지에서 복호한 CNT값이 MCC에 저장된 해당 단말기의 CNT값보다 1 큰 값인지 확인한다. 그렇지 않으면 동기화에 실패한 것으로 간주하고 단말에게 RESET 메시지를 송신하여 IV 및 CNT를 초기화한다. 이를 위해 단말과 MCC는 초기에 할당 받은 IV도 저장하고 있어야 할 것이다. 만약 동기화에 성공하면, MCC는 CNT 값을 1 증가시켜 저장하고 업데이트된 IV를 DB에 저장한다(그림 10 참조). 이렇게 함으로써 CNT는 암호화된 메시지 필드에 대하여 변조 여부를 판단할 수 있는 무결성을 지원하며, 이전에 송신된 메시지를 재전송함으로써 정상적 구조 작업을 저해하는 재생 공격도 막는다. 이로써 보안요구사항 ③을 지원한다.

비밀정보가 아닌 CNT를 암호화하는 이유는 다음과 같다. 공격자가 의도적으로 CNT는 변조하지 않고 암호화된 위치정보만 변조할 경우, MCC는 잘못된 위치정보를 얻게 된다. 뿐만 아니라 동기화 실패를 인식하지 못한 채, 변조된 암호문을 이용하여 IV를 업데이트함으로써 이후의 메시지를 제대로 복호화하지 못하게 된다.

IV. 결론 및 향후 연구

본 논문에서는 COSPAS-SARSAT 위성을 이용한 탐색 구조 단말기의 구조 신호에 사용되는 메시지 포맷을 분석하고 위치 정보와 같은 민감한 정보에 대한 암호화 가능성, 그리고 이러한 암호화 서비스 제공 시 사용될 암호키의 안전한 저장 및 처리 방식 등에 대한 새로운 방법을 제안하였다. 제한된 메시지 포맷으로 인하여 AES를 이용한 CFB 운용 모드 방식을 채택하였다. 또한 단말기의 키 저장관리 기법 및 IV의 동기화를 기법과 위치 정보에 대한 무결성 제공 및 재생 공격 방지 방안을 제시하였다. 이로써 기존 COSPAS-SARSAT의 메시지 포맷을 준수하면 탐색구조 신호에 요구되는 보안요구사항을 지원한다.

본 논문에서 제안한 방법은 COSPAS-SARSAT 메시지 포맷의 제약으로 인하여 강도 높은 보안 레벨을 제공하지는 못한다. 특히 단문 메시지 포맷을 사용하는 경우에는 위치정보의 정밀도도 낮을 뿐 아니라 메시지의 무결성이나 IV의 동기화를 제공하지 못하기 때문에 장문 메시지 포맷의 사용을 권장한다.

만약 좀 더 보안 보안 레벨을 높일 수 있는 탐색구조 메시지 보안이 요구된다면, 단말기 등록, 단말의 사용자 인증이나 장기적 키의 업데이트를 지원할 수 있도록 업링크 메시지 뿐만 아니라 위성으로부터의 다운링크 메시지를 포함한 위성 메시지 시스템을 새로 설계하는 것이 바람직하다.

REFERENCES

[1] COSPAS SARSAT, "Specification for COMPAS-SARSAT 406 MHz distress beacons," C/S T.101, Issue 3 - Revision 13, 2012.
[2] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography*, 5th Ed., CRC Press, 1996.
[3] IEEE, "Standard for cryptographic protection of data on block-oriented storage services," IEEE P1619/D16, 2007.
[4] W. Stallings, *Cryptography and Network Security*, 5th Ed., Pearson, 2011.
[5] FIPS-197, "Advanced encryption standard (AES)," 2001.

백 유 진

1997년 서울대학교 수학과(학사). 1999년 서울대학교 수학과(석사). 2003년 서울대학교 수리과학부(박사). 2003년~2003년 KAIST 박사후 연구원. 2003년~2013년 삼성전자 책임 연구원. 2013년~현재 우석대학교 정보보안학과 교수. 관심분야는 부채널 공격, 정보 보안.

조 태 남

1986년 이화여자대학교 전자계산학과(학사). 1988년 이화여자대학교 전자계산학과(석사). 2004년 이화여자대학교 컴퓨터학과(박사). 1988년~1996년 한국전자통신연구원 선임연구원. 2005년~현재 우석대학교 정보보안학과 교수. 관심분야는 암호프로토콜, 네트워크 보안, 안드로이드 보안.

김 재 현

2005년 한양대학교 전자전기컴퓨터공학부(학사). 2007년 한양대학교 전자통신컴퓨터공학과 졸업(석사). 2007년~현재 한국전자통신연구원 위성항법연구실 선임연구원. 관심분야는 위성항법, 신호처리, 무선통신.

이 상 욱

1988년 연세대학교 천문기상학과 졸업(학사), 1991년 Auburn 대학교 항공우주공학과 졸업(석사). 1994년 Auburn 대학교 항공우주공학과 졸업(박사). 1993년~현재 한국전자통신연구원 위성항법연구실 책임연구원. 관심분야는 위성시스템 및 제어, 위성항법, 탐색구조시스템.

안 우 근

2001년 고려대학교 전기전자전파공학부(학사). 2003년 KAIST 전기 및 전자공학과(석사). 2010년 KAIST 전기 및 전자공학과(박사). 2011년~현재 국방과학연구소 항법기술부 선임연구원.