민간 위성항법 메시지 인증 방안

조태남*, 용승림, 정원찬, 이상욱, 유준규
우석대학교, 인하공업전문대학, 한국전자통신연구원, 한국전자통신연구원, 한국전자통신연구원
*tncho@ws.ac.kr, slyong@inhatc.ac.kr, wcjung@etri.re.kr, slee@etri.re.kr, jgryurt@etri.re.kr

Authentication for Civil Navigation Message

Taenam Cho*, Seunglim Yong, Wonchan Jung, Sanguk Lee and Ryu Joon Gyu
Woosuk Univ., Inha Tech. College, ETRI, ETRI and ETRI

요 약

우리나라에서도 GPS와 같은 위성항법시스템으로부터 수신한 위치와 시간 정보 등을 이용한 다양한 서비스들이 이용되고 있으며 향후 더욱 많은 서비스 영역에서 활용될 것이다. 그러나 이 개방 신호에 대한 공격들이 가능하다는 것이 여러 실험에서 입증되었으며 실제 공격도 발생하였다. 항공기나 선박, 그리고 자율 자동차 등과 같은 활용영역에서 공격자가 위변조한 신호를 수신자에게 보낸다면 납치나 사고 등 매우 위험한 상황을 초래할 수 있다. 본 논문에서는 우리나라 차세대 위성의 민간 항법 신호에 대하여 공격자의 위변조된 신호가 아니라 위성에서 보내온 정당한 신호임을 인증할 수 있는 방안을 제시한다.

Ⅰ. 서 론

우리가 사용하고 있는 GPS와 같은 위성항법시스템은 인공위성이 전송하는 정보를 이용하여 단말기가 자신의 위치를 결정할 수 있도록 해주는 체계이다. 실생활과 밀접한 다양한 분야에서 활용되고 있으며, 특히 긴급 구조 호출, 헬스케어, 자율 주행, 유료도로 요금 계산 등 LBS (Location Based Service) 분야에서 많이 활용되고 있다. 만약 위치와 시간을 계산하기 위해 사용하는 위성 신호를 공격자가 위변조하여 보낸다면, 생활의 불편을 넘어 금전적 피해와 안전을 위협할 수 있으며 국가적인 범죄에도 사용될 수 있다. 이러한 공격의 가능성을 보여준 다양한 실험이 존재할 뿐만 아니라[1], 실제 전 세계적으로 수십건의 공격이 발생하고 있으며 우리나라에서도 북한이 GPS를 교란시키는 사건이 발생하기도 하였다.[2]

이에 따라 유럽의 위성항법시스템인 Galileo에서는 민간 항법신호의 인증을 지원할 예정이며 테스트가 완료된 상태이다.[3] 미국의 GPS에서도 인증 서비스를 고려하고 있으며[4], 일본의 QZSS나[5] 중국의 BeiDou를[6] 대상으로 하는 인증 기법들도 연구되고 있다.

본 연구에서는 우리나라에서 추진하고 있는 자체적인 위성항법시스템에서 인증 서비스를 고려한 위성항법 체계를 기반으로 인증 방식을 제안하고자 한다.

Ⅱ. 사전 연구

1. 위성항법 메시지 인증 방식 현황

항법신호의 인증 기법은 메시지 레벨과 신호레벨에서 이루어질 수 있다. 본 연구에서는 메시지 레벨에서의 인증기법을 연구하였다. 인증 기법들은 모두 공개키 암호, 비밀키 암호, 그리고 해시함수 등 암호기술을 이용한다. Gailleo, GPS, QZSS나 BeiDou를 대상으로 하는 항법메시지 인증 기법들은 크게 두 가지로 분류할 수 있다. 첫 번째는 Galileo에서 채택한 비밀키 암호를 이용한 MAC (Message Authentication Code)을 이용하는 방식이다. 두 번째는 GPS, QZSS와 BeiDou에서와 같이 전자서명을 이용한 방식이다. 전자서명을 이용한 방식은 비교적 간단하지만, 계산시간이 오래 걸릴 뿐만 아니라 인증정보가 많은 비트를 요구한다. 메시지 길이와 전송시간의 제약이 많은 위성항법 메시지에 적용하기 위해 비트 길이를 줄이면 그만큼 안전도가 저하된다.

2. 암호 기술

키해시함수(keyed hash function)는 임의의 길이의 데이터와 비밀키를 입력으로 하여 일정한 길이의 난수를 출력하는 함수로서, 역계산이 불가능하며 비밀키를 소유한 자만이 계산이 가능하다.[7] 전자서명은 공개키 암호알고리즘을 이용한다. 서명자가 소유한 <공개키, 개인키> 쌍 중에서 서명자만이 소유한 개인키와 데이터를 서명 알고리즘의 입력값으로 사용하여 서명값을 생성한다. 개인키에 대응되는 공개된 공개키를 이용하면 누구나 해당 데이터에 대한 서명을 검증할 수 있다.

TESLA는[8] 지연된 인증을 제공하는 네트워크 인증 프로토콜이다. 송신자가 초기비밀값 K_n에 키해시함수 $H_1()$를 반복적으로 적용하여 키체인 $K_{n-1}, K_{n-2}, ..., K_1 (H_1(K_i) = K_{i-1})$을 생성하고, K_1을 루트키(Root Key)로서 공개한다. $K_2, K_3, ..., K_n$ 순서로 데이터 M_i에 대한 인증값 $MAC_i = H_2(M_i, K_i)$를 계산하기 위한 비밀키로 사용한다. 수신자는 수신한 (M_i, MAC_i, K_{i-1})로부터 $H_1(K_i) = K_{i-1}$인지를 검사하여 키를 확인하고 $H_2(M_{i-1}, K_{i-1}) = MAC_{i-1}$인지 검사함으로써 M_{i-1}를 인증한다.

Ⅲ. 본론

본 논문에서는 한국전자통신연구소에서 설계한 차세대 위성항법 메시지 EPSM에[9] 대하여 TESLA 기반의 인증 기법을 제안한다. EPSM은 E1B채널을 통해 120bps로 전송되며 그림 2와 같이 4개의 서브프레임으로 구성된다. 각 서브프레임은 1~4의 값을 가지는 Sub_ID 필드로 구분된다. 서브프레임 1, 2($SF1, SF2$)는 핵심 항법데이터로 구성되고 서브프레임 3, 4($SF3, SF4$)는 보정데이터로 구성된다.

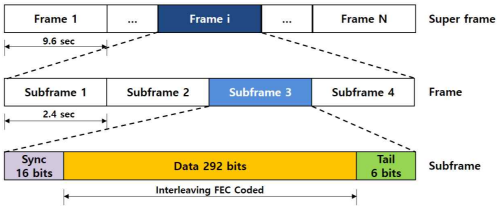

그림 1. EPSM 포맷

키체인은 160비트 SHA1[10] 사용을 가정하였으며, TESLA 루트키는 ECDSA-224[11] 전자서명과 함께 항상 브로트캐스트하여 언제든 사용자가 항법데이터 루트키를 얻을 수 있도록 한다. 인증의 효율성을 위하여 데이터의 중요도를 고려하여 세 번의 $(SF1, SF2)$ 쌍을 전송한 후에 한번의 $(SF3, SF4)$를 전송한다. 2개의 서브프레임 전송 후에는 1개의 인증 프레임을 전송한다. 인증 프레임을 $A1$, ..., $A8$이라고 했을 때 전송 순서는 그림 2와 같다. 인증프레임 $A4, A8$에는 루트키 정보만 들어 있고, $A1, A2, A3, A5, A6, A7$에는 $(SF1_i, SF2_i)$에 대한 인증정보 MAC_i와 이전 키 K_{i-1}가 들어 있다. MAC_i는 HMAC-SHA1$(SF1_i, SF2_i, K_i)$을 수행한 결과의 LSB 23비트이다. $(SF1_i, SF2_i, A_i)$를 받은 수신자는 버퍼링 했다가 다음 서브프레임 세트를 $(SF1_{i+1}, SF2_{i+1}, A_{i+1})$받았을 때, A_{i+1}에 포함된 키 K_i를 키를 확인한 후 HMAC-SHA1$(SF1_i, SF2_i, K_i)$를 계산하여 A_i에 포함된 MAC_i와 같은지 비교함으로써 $(SF1_i, SF2_i)$를 인증한다.

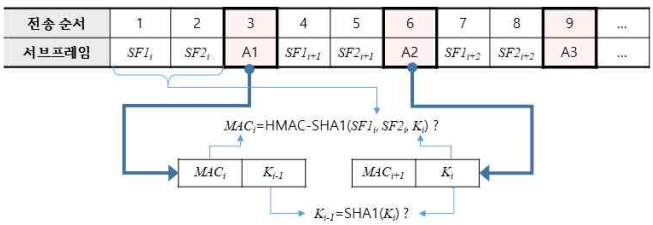

그림 2. 인증프레임의 키와 MAC 관계

인증프레임의 비트 구성은 표 1과 같다. 루트키 정보는 8개 인증정보에 분할되어 전송된다. 8개 인증 프레임에서 해당 비트 길이만큼씩의 MSB를 연결하면 루트키와 루트키에 대한 인증정보를 얻을 수 있다. 200비트 LSB인 MAC 정보는 해당 인증프레임 앞에 전송된 $(SF1, SF2)$에 대한 인증정보와 이전 키값이다. 그림 3은 8개 인증프레임의 구체적인 구성 필드를 보여주고 있다.

표 1. 인증 서브프레임의 비트 구성

Sub_ID	17 (A1)	18 (A2)	19 (A3)	20 (A4)	21 (A5)	22 (A6)	23 (A7)	24 (A8)	Total Bits
Root Key	30	30	30	230	30	30	30	230	640
MAC	200	200	200		200	200	200		

Ⅳ. 결론

본 논문에서는 한국전자통신연구원에서 설계한 차세대 위성항법 메시지에 대하여 TESLA 방식을 이용한 인증 방식을 제안하였다. 무료로 제공되는 민간 신호에 대한 인증은 향후 더욱 다양화될 서비스들의 안전성 제공에 활용될 수 있을 것으로 사료된다. 안전성을 더 강화하고자 한다면 인증정보의 비트길이가 길어지고 인증 시간이 길어지게 된다. 사용자의 편의성과 안전성 간의 trade-off와 타 위성과의 연동 등 다양한 서비스 환경을 고려한 좀 더 정교한 인증방식에 대한 연구가 진행되어야 할 것이다.

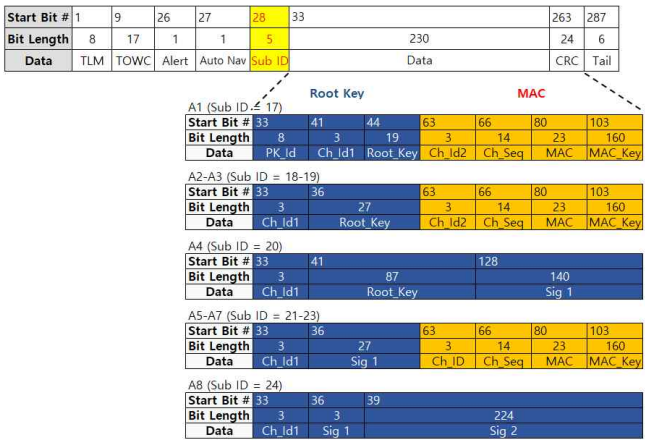

그림 3. EPSM의 인증 서브프레임 구조

ACKNOWLEDGMENT

본 논문은 2021년도 한국전자통신연구원 연구운영비지원사업의 재원으로 수행하고 있는 한국전자통신연구원의 연결의 한계를 극복하는 초연결 입체통신 기술 연구 (21ZH1100) 과제의 위탁연구과제의 연구결과이다.

참 고 문 헌

[1] A. J. Kerns, D. P. Shepard, J. A. Bhatti and T. E. Humphreys, "Unmanned Aircraft Capture and Control Via GPS Spoofing," Journal of Field Robotics, vol. 31, no. 4, pp.617-636, 2014.

[2] 중앙일보, "북한, GPS 교란 공격 … 키 리졸브 훈련 방해 노렸나", 2011 (https://news.joins.com/article/5149695).

[3] European Commission, Tests of Galileo OSNMA underway, Feb., 2021 (https://ec.europa.eu/defence-industry-space/tests-galileo-osnma-underway-2021-02-11_en).

[4] Air Force Research Laboratory (AFRL) Space Vehicles Directorate, Advanced GPS Technology, "Chips Message Robust Authentication (Chimera) Enhancement for the L1C Signal: Space Segment/User Segment Interface," IS-AGT-100, April 2019.

[5] Dinesh Manandhar, Ryosuke Shibasaki, "Authenticating GALILEO Open Signal Using QZSS Signal," ION GNSS+ 2018, pp.3995-4003, Sept. 2018.

[6] Zhijun Wu, Yun Zhang, and Rusen Liu, "BD-II NMA&SSI: An Scheme of Anti-Spoofing and Open BeiDou II D2 Navigation Message Authentication," IEEE Access, Vol. 8, 2020.

[7] H. Krawczyk, M. Bellare and R. Canetti, "HMAC: Keyed-Hashing for MessagevAuthentication," Network Working Group, 1997.

[8] A. Perrig, R. Canetti, J. Tygar and D. Song, "Efficient Authentication and Signing of Multicast Streams over Lossy Channels," IEEE Symposium on Security and Privacy, pp.56-73, May 2000.

[9] Sangwook Lee, et. al., "Prototyping of Signal Generator for Satellite Navigation Payload," Electronic Telecommunications Research Institute TD, Jan. 2021.

[10] NIST, FIPS PUB 180-1, National Institute of Standards and Technology, 1994.

[11] Public key cryptography for the financial services industry: The elliptic curve digital signature algorithm (ECDSA), ANSI, X9.62-1998, approved Jan. 1999.