논문 22-47-05-04 The Journal of Korean Institute of Communications and Information Sciences '22-05 Vol.47 No.05
https://doi.org/10.7840/kics.2022.47.5.731

위성항법 메시지 및 위성항법 정밀보정메시지 인증

조 태 남°, 용 승 림*, 정 원 찬**, 이 상 욱**, 유 준 규**

Authentication Scheme for Satellite Navigation Message and Precision Correction Message

Taenam Cho°, Seunglim Yong*, Wonchan Jung**, Sanguk Lee**, Ryu Joon Gyu**

요 약

우리는 미국의 범지구위성항법시스템인 GPS로부터 위치 및 시간 정보를 수신하여 네비게이션 등에서 사용하고 있으나 수십미터 오차를 가진다. 항공이나 자율주행 등 정밀한 위치 정보가 필요한 경우에는 오차를 보정하기 위한 정밀보정 서비스가 필요하기 때문에 해외에서도 정밀도를 높이기 위한 서비스를 준비하고 있다. 반면, 위성항법메시지에 대한 스푸핑 공격은 항공, 선박 등의 위치를 교란시킴으로써 사회·경제적 혼란과 피해를 야기시킬 수 있다. 점차 다양해지고 정밀해진 GNSS에 대한 공격은 정밀보정 서비스에서 더욱 치명적일 수 있기 때문에 위성메시지 인증에 대한 연구가 필요하다. 인증 방식은 각 GNSS 전송속도나 메시지 구조 등 그 특성에 따라 달라질 수밖에 없기 때문에 각국의 GNSS에 대한 인증연구가 이루어지고 있다. 본 논문에서는 우리나라에서 추진하고 있는 KPS에 적용될 수 있는 민간용 위성항법 데이터와 정밀보정 메시지에 대한 인증 방안을 제시한다.

키워드 : 위성항법시스템, KPS, 정밀보정 서비스, 메시지 인증, 보안
Key Words : GNSS, KPS, Precision Correction Service, Message Authentication, Security

ABSTRACT

We receive location and time information from the GPS, the US global satellite navigation system, and use it for navigation, but it has an error of several tens of meters. When precise location information is required, such as in aviation or autonomous driving, precision reinforcement services are required to correct errors, so services with high accuracy are being prepared overseas. Spoofing attacks on these satellite navigation messages can cause social and economic chaos and damage by disturbing the positions of air and ships. Since attacks on GNSS, which have become increasingly diversified and sophisticated, can be more lethal in the precision correction service, research on satellite message authentication is needed. Since the authentication method inevitably varies depending on the characteristics of each GNSS transmission speed or message structure, etc., research on GNSS authentication is being conducted in each country. In this paper, we propose authentication methods for civilian satellite navigation data and precision reinforcement messages that can be applied to the KPS, which is being promoted in Korea.

※ 본 연구는 2021년도 한국전자통신연구원 연구운영비지원사업의 재원으로 수행하고 있는 한국전자통신연구원의 연결의 한계를 극복하는 초연결 입체통신 기술 연구 (21ZH1100)의 지원으로 수행한 정밀 보강 위성항법 서비스 사용자 인증방법 연구 과제의 결과입니다.
°• First and Corresponding Author : Woosuk University Department of IT & Electronics Engineering, tncho@woosuk.ac.kr, 정회원
* Inha Tech. College, slyong@inhatc.ac.kr
** Electronics & Telecommunications Research Institute, wcjung@etri.re.kr, 정회원; slee@etri.re.kr, 정회원; jgryurt@etri.re.kr, 정회원
논문번호 : 202112-341-A-RE, Received December 29, 2021; Revised February 22, 2022; Accepted February 28, 2022

Ⅰ. 서 론

우리가 사용하고 있는 위성항법 시스템은 지구 궤도상에 다수의 위성으로 구성된 위성군으로부터 수신되는 위성의 위치정보와 전파를 이용한 거리측정을 통하여 3차원의 위치 및 시각 동기 정보를 제공하는 위성시스템이다[1]. 위성은 위성에 탑재된 원자시계의 시간 값과 현재 위치 값을 전송하고 사용자의 수신기는 수신기의 시간 값과의 시간차를 통해 위성과의 거리를 알아낸다.

GNSS(Global Navigation Satellite System)를 이용한 다양한 서비스가 제공되고 있으나 위성 신호가 도달하는 데 걸리는 시간을 기준으로 이 거리를 측정하기 때문에 수십 억분의 1초의 오차로 인해 적지 않은 오차가 생길 수 있다. GPS(Global Positioning System)의 경우 최대 오차는 수직 20m, 수평 10m라고 알려져 있다[2]. 특히 항공이나 선박 운항, 해양 탐사, 인명 구조 혹은 자율 주행 자동차 등에서는 좀 더 보강되어 정밀한 위치를 계산할 수 있어야하기 때문에 이러한 오차는 심각한 영향을 미칠 수 있다. 국내외에서 GNSS의 오차를 보정하여 정밀도를 높이기 위한 서비스를 제공하고 있다.

한편, 위성항법시스템에 대한 스푸핑(spoofing)과 같은 공격은 수신기가 자신의 위치를 실제 위치와 다르게 인식하거나 공격자가 결정한 다른 시간으로 착각하게 할 수 있다. 이러한 공격은 신호 조작으로 인한 사회적 혼란을 야기하고 경제적 피해 규모를 확대시킬 수 있으며 특정 타겟을 대상으로 한 생활의 불편, 금전적 피해, 개인 안전에도 위협이 될 수 있다[3]. 이를 위하여 민간 사용자 보호를 위한 다양한 위성 신호 인증 방식이 연구되고 있다. 유럽의 Galileo는 메시지 인증 서비스를 시험운영중이며 미국의 GPS도 지원 예정이다. 그 밖에 중국의 BeiDou와 일본의 QZSS 및 향후 개발될 우리나라 KPS(Korean Positioning System)에 대한 연구도 진행되고 있다. 그러나 아직 정밀보정 서비스의 신호에 대한 인증 연구는 이루어지지 않고 있다.

본 논문에서는 우리나라에서 추진하고 있는 KPS에 적용될 수 있는 민간용 위성항법 메시지와 정밀보정 메시지를 함께 인증할 수 있는 방안을 제시한다. Ⅱ장에서 위성항법의 서비스 현황을 살펴보고 Ⅲ장에서는 인증에 사용되는 암호기술의 개념에 대해 기술한다. Ⅳ장에서는 본 연구에서 제안하는 인증 기법을 제안하고 Ⅴ장에서는 제안 기법에 대한 분석과 비교를 하며 Ⅵ장에서 결론을 맺는다.

Ⅱ. 위성항법시스템 서비스 현황

위성항법메시지(NAV: NAVigation message)에 대한 인증 서비스는 여러 나라에서 연구되고 있다. 위성에 기반한 정밀보정 서비스(CLS: Centimeter Level Service message)도 서비스를 계획하고 있지만 아직 인증에 대한 연구는 진행되고 있지 않다.

2.1 위성항법시스템 인증 기술

유럽 연합의 Galileo[4]는 125bps 전송속도를 가지는 E1B 채널로 전송되는 I/NAV 메시지 에 대하여 인증 서비스를 시범운용하고 있다. 이 방식에서는 메시지를 이루는 각 페이지에 대하여 TESLA(Timed Efficient Stream Loss-tolerant Authentication)[5] 기법을 이용하여 인증하며, 사용되는 해시함수와 루트키를 안전하게 배포하기 위한 디지털 서명 방식은 선택할 수 있다.

미국의 GPS[6-8]에 대한 인증 방식으로서 제안된 Chimera(Chips Message Robust Authentication)는 100bps 전송속도를 가지는 CNAV-2 L1C 채널로 전송되는 항법메시지와 확산코드(spreading code)에 대하여 디지털 서명으로 인증한다.

중국의 BeiDou 중궤도와 경사궤도 위성은 50 bps로 전송되는 D1 메시지 포맷을 사용하고, 정지궤도 위성은 500 bps로 전송되는 D2 메시지 포맷을 사용한다[9]. Zhijun Wu 등이 제시한 방식에서는[10] 항법데이타에 대한 디지털 서명값을 생성하고 특정 메인프레임에 실어보낸다. D1 메시지에서는 5개 서브프레임 중 1-3번 서브프레임에 항법데이터가 전송된다. 또한 Zhijun Wu 등이 제안한 방식에서는[11], 500bps로 전송되는 D2 메시지에 대하여 그룹 인증정보와 페이지 인증정보를 대칭키로 암호화하여 분할전송하고, 항법데이터에 대해서는 디지털 서명 방식을 사용한다.

Dinesh Manandhar 등은[12] 일본의 QZSS 뿐만 아니라 수신가능한 모든 위성으로부터의 항법 데이터를 인증할 수 있는 방법을 제안하였다. ADC(Authentication Data Center)에서 QZSS L1C/A, GPS L1C/A 및 갈릴레오 E1B 신호로부터 항법 데이터를 수신하고 추출한 항법데이터에 대한 인증정보를 생성한 후, QZSS 항법데이터를 대체하여 위성을 통해 브로드캐스트한다.

국내에서는 KPS에 적용될 수 있는 항법메시지[12,13]에 대하여 TESLA 방식을 이용한 인증기법이 제안되었다[14,15].

2.2 정밀 보정 서비스 현황

세계적으로 이미 위성기반 정밀보정 서비스가 운영되고 있거나 예정되고 있다.

Galileo HAS(High Accuracy Service)는 사용자의 개선된 사용자 위치 정보 보정을 위하여 고정밀 보정 정보를 전 세계에 무료로 제공하고 있으며 2데시미터 미만의 정확도로 실시간 개선된 사용자 포지셔닝 성능을 제공한다. Galileo HAS는 제공 범위에 따라 2가지의 수준으로 구성된다. 서비스 수준 1은 전 세계에 적용되는 서비스로 Galileo E1/E5b/E5a/E6 및 E5AltBOC 및 GPS L1/L5/L2 신호에 대한 고정밀 보정 데이터를 제공한다. 서비스 수준 2는 유럽 적용 범위(ECA)에 걸친 지역 적용 범위에서 SL1 보정에 추가적 데이터를 제공한다[16].

QZSS는 서브미터 레벨 서비스(SLAS: Submeter Level Augmentation Service)와 센티미터 레벨의 서비스(CLAS: Centimeter Level Augmentation Service)를 제공하고 있다. CLAS는 GPS, Galileo 그리고, QZSS 위성군에 대한 보정정보를 제공한다. 일본 지리정보국(Geospatial Information Authority)의 GNSS 기반 관제소에서 얻은 데이터를 사용하여 고정밀 측위 정보를 생성한다[17].

BeiDou는 GEO-3 위성을 이용하여 정밀보정 서비스를 제공할 예정이다. PPP-B2b 서비스에서 BDS-GPS, BDS-GLONASS, BDS-Galileo의 위성 궤도 수정, 시계 수정 및 코드 바이어스 수정 정보가 제공될 예정이며 현재는 BDS-3 및 GPS 위성의 보정만 중국 및 그 주변 사용자에게 제공되고 있다[18].

Ⅲ. 기반 암호 기술

3.1 암호시스템(cryptosystem)

메시지를 보호하거나 인증하는데 필요한 핵심 기술은 암호기술이다. 통신에 참가하는 정당한 개체들은 소유한 키(key)값을 이용하여 메시지에 대한 안전성을 보장 받는다. 비밀키 암호방식은 송수신 개체만이 하나의 비밀키를 공유한다. AES(Advanced Encryption Standard)[19], SEED[20] 등이 대표적이다. 공개키 암호방식에서는 각 개체가 각각 자신의 공개키 PK와 개인키 RK 한쌍을 소유하는데 PK는 공개값이고 RK는 자신만 소유하는 비밀값이다. RSA(Rivest-Shamir-Adleman)[21], ECC(Elliptic Curve Cryptography)[22] 등이 대표적이다.

3.2 해시함수(hash function)

보안에서 사용되는 해시함수는 일방향성(one-wayness), 충돌회피성(collision resistent)과 같은 몇 가지 엄격한 조건을 만족하는 함수로서, 입력 메시지 m에 대하여 일정한 비트 길이의 값을 산출한다. 일반적으로 입력 메시지보다 해시함수값이 짧기 때문에 메시지를 축약하는데 사용된다. 대표적인 해시함수는 SHA1(Secure Hash Algorithm 1)[23], SHA2[24] 등이 있으며, 산출되는 해시값의 비트 길이가 길수록 안전하다.

3.3 메시지 인증(message authentication)

메시지에 대한 인증 방식은 대칭키 암호를 이용하는 방식들과 공개키 암호를 이용하는 방식들이 있다. 위성항법메시지 인증에 사용되는 대칭키 인증 방식은 유럽의 Galileo에 적용한 TESLA[4,5]가 대표적이며, 공개키 인증방식은 미국의 GPS[6] 등에 적용한 ECDSA(Elliptic Curve Digital Signature Algorithm)[25] 디지털 서명 방식이 대표적이다[7,8]. TESLA는 대칭키 암호를 이용하기 때문에 계산 속도가 빠르지만, 키공유의 문제를 해결하기 위하여 다소 복잡한 프로토콜로 설계된다. 디지털 서명 방식은 계산 속도가 느리고 PKI(Public Key Infrastructure)가 전제되어야 하지만 인증 프로토콜이 간단하고 전송 정보가 적다.

본 논문에서 제안하는 방식에서는 디지털 서명을 이용한다. 메시지를 m, 서명 알고리즘을 $S()$, 검증 알고리즘을 $V()$라고 할 때, m에 대한 서명값 Sig는 m를 해시함수 $H()$에 적용하여 축약한 후 서명자의 개인키 RK를 이용하여 (1)과 같이 계산된다.

$$Sig \leftarrow S(H(m), RK) \tag{1}$$

(m, Sig)를 수신한 개체는 메시지를 해시한 후 서명자의 공개키 PK를 이용하여 (2)과 같은 방법으로 계산하고, 그 결과값에 따라 서명의 유효성을 검증하고 메시지의 무결성(integrity)을 인증한다.

$$V(H(m), PK, Sig) = Success\ ? \tag{2}$$

공개키 암호를 이용한 대표적인 디지털 서명 알고리즘으로는 RSA[21], DSS(Digital Signature Standard)[26], ECDSA[25], KCDSA(Korean Certificated-based Digital Signature Algorithm)[27] 등이 있다. 안전성의 척도인 보안 강도는 서명에 사용되는 개인키의 길이가 길수록 향상된다.

Ⅳ. 인증 방안 제안

일반적으로 위성항법 메시지는 전송속도가 느린 채널을 이용한다. 본 논문에서는 항법메시지와 정밀보정 메시지에 대한 인증을 속도가 빠른 정밀보정 메시지를 통해 수행하는 방식에 대하여 연구하였다.

4.1 항법메시지 구조

한국전자통신연구원에서는 차세대 위성으로서 신호생성기 및 위성항법메시지 구조를 설계하였다[12,13].

1개의 항법메시지 프레임은 4개의 서브프레임으로 구성되고, 각 서브프레임은 그림 1과 같이 동기화를 위한 16비트 Sync, 항법메시지 292비트 Data part, 그리고 6비트 Tail로 구성되어 12초에 걸쳐 전송된다. Data part에는 TLM, Sub ID, CRC 등이 4개 서브프레임에 공통적으로 포함되고 나머지 233비트는 서브프레임별로 다른 항목으로 구성된다. 본 논문에서는 233비트 중에 포함된 3비트의 spare 비트를 인증을 위한 일련번호 Seq로 사용한다. 이 값은 0~7값을 가질 수 있으므로 12초*8=96초마다 순환된다.

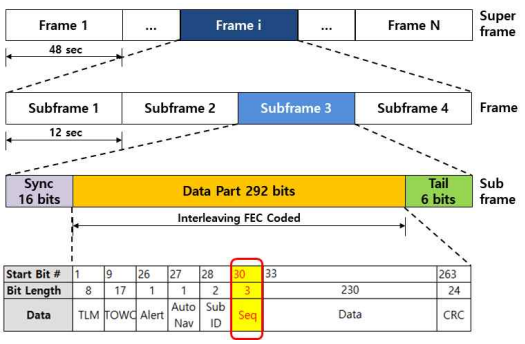

그림 1. NAV 메시지 포맷
Fig. 1. NAV message format

4.2 정밀보정 메시지 구조

설계가 가장 구체화되어 있는 일본의 QZSS의 CLAS 메시지는[17] L6 대역대를 이용하여 2000bps로 서비스한다. 본 연구에서는 이 메시지 구조에 기반하여 인증 방식을 설계하였다. 메시지 구조는 그림 2와 같이 하나의 메시지는 6개의 서브프레임으로 구성된다. 각 서브프레임은 기존의 5개의 1695비트 Data part와 인증을 위해 본 연구에서 추가한 1개의 Data part로 구성된다. 각 Data part에는 49비트 헤더와 256비트 Reed-Solomon 코드가 추가되어 전송된다.

49비트 헤더에는 그림 3과 같이 위성을 식별할 수 있는 PRN과 메시지 식별자 ID가 포함되어 있다.

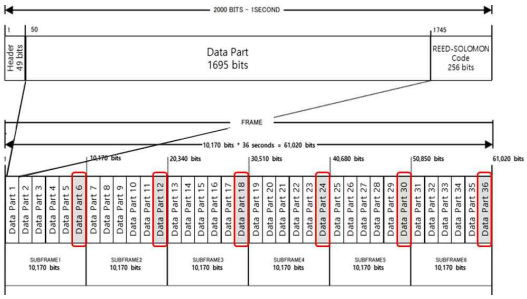

그림 2. CLS 메시지 포맷
Fig. 2. CLS message format

그림 3. CLS 메시지 헤더
Fig. 3. CLS message header

각 Data part를 구성하는 항목은 Subtype에 따라 달라진다. 가장 먼저 전송되는 Subtype 1 (Compact SSR Mask)에는 이후에 전송되는 정밀보정 데이터에 대한 정보를 제공하는 헤더의 역할을 한다. 즉, 이후 전송되는 보정 정보가 어떤 위성의 어떤 신호에 대한 데이터인지를 알려준다. 그림 4와 같이 Header에는 반복되는 GNSS 개수(No. of GNSS)가 포함되어 있고, 그 수만큼 향후 송신할 데이터에 해당하는 위성과 신호에 마스크 정보가 들어있다.

Subtype 1에 담긴 정보에 따라 그림 5와 같이 Subtype 메시지들이 전송된다. 각 서브프레임의 6번째로 전송되는 Subtype 15에 본 연구에서 추가 정의한 인증 정보가 포함되도록 설계하였다.

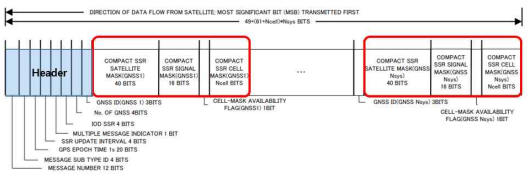

그림 4. Type 1 구조
Fig. 4. Structure of Subtype 1

4.3 인증용 Subtype 15

4.3.1 인증 정보 전송 방안

4.1절에 기술한 항법메시지는 12초마다 서브프레임이 전송되고, 4.2절에 기술한 정밀보정 메시지는 6초마다 서브프레임이 반복되므로 그림 6과 같이 두

SF	Sec							
1	1	Header	ST1	ST3	ST2		ST4	RS
	2	Header	ST4	ST7	ST6		ST1	RS
	3	Header	ST12					RS
	4	Header	ST12		ST6		ST12	RS
	5	Header	ST12			ST11	RSVD	RS
	6	Header	ST15					RS
2	7	Header	ST3	ST		ST12		RS
	8	Header	ST12					RS
	9	Header	ST12				ST6	RS
	10	Header	ST12					RS
	11	Header	ST12			ST11	RESERVED	RS
	12	Header	ST15					RS
3	13	Header	ST3	ST6		ST12		RS
	14	Header	ST12				ST6	RS
	15	Header	ST6	ST12				RS
	16	Header	ST12					RS
	17	Header	ST12		ST11	RESERVED		RS
	18	Header	ST15					RS
4	19	Header	ST3	ST6		ST12		RS
	20	Header	ST12					RS
	21	Header	ST12	ST6		ST12		RS
	22	Header	ST12					RS
	23	Header	ST12		ST11	RESERVED		RS
	24	Header	ST15					RS
5	25	Header	ST3	ST6		ST12		RS
	26	Header	ST12				ST6	RS
	27	Header	ST6	ST12				RS
	28	Header	ST12					RS
	29	Header	ST12	ST11	RESERVED			RS
	30	Header	ST15					RS
6	31	Header	ST3	ST6		ST12		RS
	32	Header	ST12					RS
	33	Header	ST12	ST11		ST6		RS
	34	Header	ST6		ST12			RS
	35	Header	ST12		RESERVED			RS
	36	Header	ST15					RS

그림 5. Subtype 전송 스케줄
Fig. 5. Transmission schedule of Subtypes

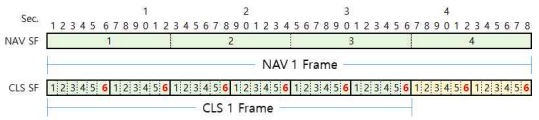

그림 6. 항법메시지와 정밀보정 메시지의 동기화
Fig. 6. Synch. of Navigation message and CLS message

메시지는 12초마다 동기화된다. 정밀보정 메시지의 각 서브프레임의 6번 Data part에 인증 정보(디지털 서명)를 전송하는 2가지 방안을 제안한다.

항법메시지에 대한 디지털 서명값과 정밀보정 메시지에 대한 디지털 서명값을 각각 Sig_{NAV}와 Sig_{CLS}라고 하자. 인증 방안 1은 그림 7과 같이 홀수번째 서브프레임에는 해당 정밀보정 메시지 서브프레임의 1~5번 Data part에 대한 디지털 서명값인 Sig_{CLS}을 전송하고, 짝수번째 서브프레임에는 Sig_{CLS}와 함께 이 서브프레임과 동기화된 항법메시지에 대한 디지털 서명값인 Sig_{NAV}를 전송하는 방식이다.

인증 방안 2는 그림 8과 같이 짝수번째 서브프레임에는 이 서브프레임과 동기화된 항법메시지에 대한 디지털 서명값인 Sig_{NAV}를 보내고, 홀수번째 서브프레임에는 해당 정밀보정 메시지 서브프레임과 이전 서브프레임의 1~5번 Data part들에 대한 디지털 서명값인 Sig_{CLS}을 전송하는 방식이다.

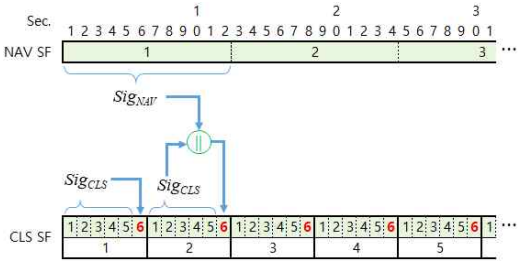

그림 7. 인증 방안 1
Fig. 7. Authentication method 1

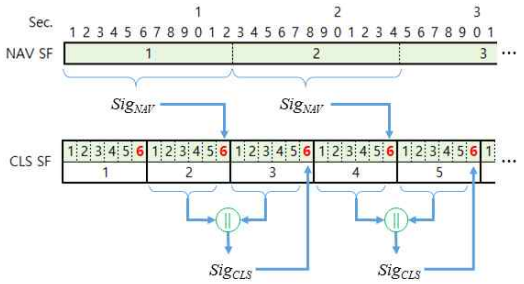

그림 8. 인증 방안 2
Fig. 8. Authentication method 2

이 두 가지 방식은 안전성을 좌우하는 디지털 서명키의 길이에 따라 채택할 수 있다. 인증용 Subtype 15의 필드 구성은 표 1과 같다. $Auth\,Tgt$은 인증 대상을 나타낸다. 값이 0일 경우는 인증 방안 2의 처음 시작 서브프레임일 경우와 같이 인증 정보가 없는 경우이다. NH는 $Auth\,Tgt$이 1 혹은 3일 경우 인증 대상

표 1. Subtype 15 필드 구성
Table 1. Fields of Subtype 15

Field	Bit Length	Meaning and Value
$Auth\,Tgt$	2	Authentication Target 0: None, 1: NAV, 2: CLS, 3: NAV+CLS
NH	32	NAV header
HID	4	Hash algorithm ID (Ref. Table 5)
SID	1	Signature algorithm ID 0: ECDSA, 1: EC-KCDSA
$KLen$	2	Bit length of signature key 0: 224, 1: 256, 2: 384, 3: 512
PID	5	Public key ID for key table (Ref. Fig. 9)
Sig_{NAV}	448, 512, 668, 1024	Digital signature for NAV
Sig_{CLS}	448, 512, 668, 1024	Digital signature for CLS

표 2. Hash ID 별 해시 함수
Table 2. Hash functions for Hash ID

Value	Hash function	Value	Hash function
0	SHA-224	8	SHA3-384
1	SHA-256	9	SHA3-512
2	SHA-384	10	LSH-224
3	SHA-512	11	LSH-256
4	SHA-512/224	12	LSH-384
5	SHA-512/256	13	LSH-512
6	SHA3-224	14	LSH-512-224
7	SHA3-256	15	LSH-512-256

이 되는 항법메시지의 헤더이다. *HID*와 *SID*는 디지털 서명에 사용된 해시 함수와 디지털 서명 알고리즘이다. *HID*는 0~15값을 가지며 한국인터넷진흥원(KISA: Korea Internet and Security Agency)에서 권고하는 16가지 해시 알고리즘으로서[28] 표 2에 나타나 있다. 서명 알고리즘으로는 가장 널리 사용되는 ECDSA와 타원곡선을 이용한 우리나라 서명 알고리즘인 EC-KCDSA(Elliptic Curve-KCDSA)를 사용한다. $KLen$은 디지털 서명 생성에 사용된 개인키의 길이를 나타낸다. 이 길이도 한국인터넷진흥원에서 권고하는 키의 길이이다. 이 값에 따라 Sig_{NAV}와 Sig_{CLS}의 길이가 결정되는데, 사용한 키 길이의 2배가 된다. *PID*는 디지털 서명의 검증에 사용될 공개키 테이블의 색인으로서 4.3.3에서 설명한다.

4.3.2 전송 방식에 따른 메시지 비트 길이

인증 방안 1의 홀수번째나 인증 방안 2에서와 같이 Sig_{NAV}나 Sig_{CLS}를 각각 사용할 때, 키 길이별 메시지의 비트길이는 표 3과 같다. 표 4는 인증 방안 1에서 Sig_{NAV}와 Sig_{CLS}를 함께 전송할 때의 비트길이를 나타낸다. Data part의 길이가 1695비트인 것을 고려할 때, 적용 가능한 비트길이를 굵은 선으로 표시하였다. 인증 방안 1의 짝수번째 디지털 서명 생성 방식은 2가지로 설계할 수 있다. 인증 방안 1-1은 Sig_{NAV}와 Sig_{CLS}에 사용되는 해시함수, 서명 알고리즘과 키 길이를 동일하게 적용하는 방안이고, 인증 방안 1-2는 서로 다른 함수, 알고리즘과 키 길이를 적용할 수 있도록 하는 방안이다.

표 3. Sig_{NAV}와 Sig_{CLS}의 비트 길이
Table 3. Bit lengths of Sig_{NAV} and Sig_{CLS}

Sig. / Field	Sig_{NAV}				Sig_{CLS}			
AuthTgt	2	2	2	2	2	2	2	2
NH	32	32	32	32				
HID	4	4	4	4	4	4	4	4
SID	1	1	1	1	1	1	1	1
KLen	2	2	2	2	2	2	2	2
PID	5	5	5	5	5	5	5	5
Sig_{NAV}	448	512	768	1024				
Sig_{CLS}					448	512	768	1024
Total bit length	494	558	814	1070	462	526	782	1038

표 4. $Sig_{NAV}+Sig_{CLS}$의 비트 길이
Table 4. Bit lengths of $Sig_{NAV}+Sig_{CLS}$

Sig_{NAV} \ Sig_{CLS}		448	512	768	1024
Auth. method 1-1		942	1070	1582	2094
Auth. method 1-2	448	954	1018	1274	1530
	512	1018	1082	1338	1594
	768	1274	1338	1594	1850
	1024	1530	1594	1850	2106

4.3.3 키 관리

해시함수 출력값의 길이뿐만 아니라 서명용 키의 길이는 안전도를 좌우한다. 공격자의 계산 능력이 점차 증가함에 따라 인터넷진흥원에서는 NIST[29] 등의 권고안을 참조하여 연도별로 서명용 키의 길이에 대한 권고안을 제시하였다[28]. 제안 방식에서 사용하는 ECDSA와 EC-KCDSA의 경우에는 2030년까지는 112비트 보안강도에 해당하는 224비트 키를 권고하며 그 이후에는 128비트 보안강도 이상인 256, 384, 512 비트 키를 권고하고 있다.

위성의 수명을 고려하여, 그림 9와 같이 서명 알고리즘(*SID*)과 키 길이(*KLen*)별로 *PID*로 식별되는 32개 공개키쌍을 가진 키테이블을 생성한다. 위성에는 서명에 필요한 개인키를 저장하고 단말기에는 검증에 필요한 공개키를 저장한다. 한국인터넷진흥원 권고안에 따르면 서명용 키의 사용기한은 최대 2년이므로 1년 주기로 갱신한다면 하나의 테이블은 32년간 사용할 수 있다. 위성 운용 및 보안 정책에 따라 통합된 하나의 테이블을 생성하거나 일부 테이블을 생성하지 않을 수도 있으며, 인증 방안 1-2와 같이 Sig_{NAV}와 Sig_{CLS}에 다른 알고리즘을 사용할 경우 그림 9와 같은 테이블을 각각 1세트씩 따로 구성할 수도 있을 것이다.

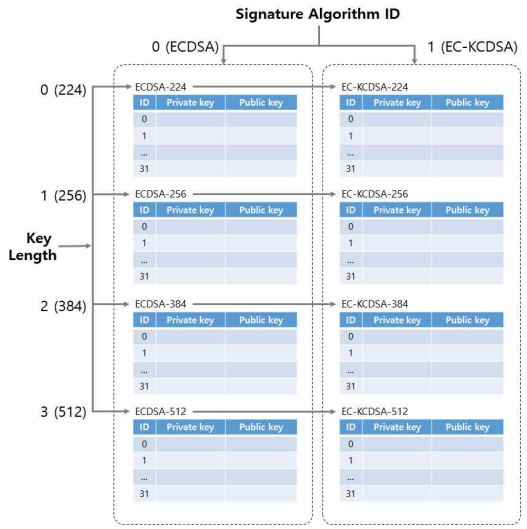

그림 9. 디지털 서명용 키 테이블
Fig. 9. Key table for digital signature

4.3.4 인증 절차

정밀보정 메시지의 Subtype 15를 수신하면 프로시져 1 및 2와 같이 인증 절차를 수행한다. 만약, 인증 방안 1-2를 사용할 경우, 프로시져 2의 3번줄 CLS는 이전 2개의 서브프레임에 해당할 것이다. 만약 마지막 단계에서 검증에 실패하면 수신한 메시지 인증되지 않은 것이므로 폐기해야 한다.

프로시져 1. 항법메시지에 대한 인증
Procedure 1. Verification for NAV message

1. $AT \leftarrow 1^{st}$ LSB of $AuthTgt$
2. If ($AT \neq 1$) return
3. $NAV \leftarrow$ Navigation message
4. If ($NH \neq$ Header of NAV) return
5. $H() \leftarrow$ Hash function specified by HID
6. $HV \leftarrow H(NAV)$
7. $V() \leftarrow$ Verification algorithm specified by SID
8. $PK \leftarrow$ Public key from key table specified by SID, $KLen$ and PID
9. Check if $V(HV, PK, Sig_{NAV})$ = success

프로시져 2. 정밀보정 메시지에 대한 인증
Procedure 2. Verification for CLS message

1. $AT \leftarrow 2^{nd}$ LSB of $AuthTgt$
2. If ($AT \neq 1$) return
3. $CLS \leftarrow$ Data part 1~5 of CLS message
4. $H() \leftarrow$ Hash function specified by HID
5. $HV \leftarrow H(CLS)$
6. $V() \leftarrow$ Verification algorithm specified by SID
7. $PK \leftarrow$ Public key from key table specified by SID, $KLen$ and PID
8. Check if $V(HV, PK, Sig_{NAV})$ = success

V. 분석 및 비교

Ⅲ장의 서두에서 기술한 바와 같이 정밀보정 서비스에 대한 인증 방식은 연구된 바가 없기 때문에 본 논문에서 제안한 인증 방식 1과 2에 대하여 분석하고 비교하였다.

5.1 성능 분석

5.1.1 성능 척도[15,30]

기존의 인증방법과 성능을 비교하기 위한 5가지 척도로서 인증시간에 관련된 TFAF와 TBA, 인증 적용에 따른 서비스 지연에 관련된 TFUD, TBUD 및 DTFAF를 도입하였다. 위성이나 수신기의 인증값 계산이나 검증에 소요되는 시간은 위성으로부터의 데이터 전송시간에 비해 미미하기 때문에 계산값에 반영하지 않았다.

(1) TFAF(Time to First Authentication Fix)
사용자가 수신기를 처음 켜거나 오랜만에 켜서, 인증 단위(예: 서브프레임)의 일부 메시지만 수신했을 경우에는 인증을 수행할 수 없다. 이 척도는 수신기를 켰을 때부터 인증된 메시지를 사용할 수 있을 때까지 소요되는 최대 시간을 의미한다.

(2) TBA(Time Between Authentication)
메시지를 인증한 후, 다음 인증까지의 최대 시간 간격을 의미한다. TFAF가 사용자가 기다려야 하는 최악의 시간이라면, TBA는 실질적인 인증 시간이라고 볼 수 있다. 따라서 TFAF 보다 짧다.

(3) TFUD(Time to First Unauthenticated Data)
추가된 인증 정보를 무시할 때 최초 메시지 수신 시간의 최대값을 의미한다. 이 시간은 인증정보를 추가하지 않았을 때의 시간에 비해 얼마나 지연이 발생하는지를 의미한다.

(4) TBUD(Time Between Unauthenticated Data)
추가된 인증 정보를 무시할 때, 연속적인 데이터 수신시간 간격을 의미한다. 인증정보 추가로 인하여 발생하는 지연시간이다.

(5) DTFAF(Delay Time to First Authentication Fix)
TFAF에는 사용할 수 없는 메시지 수신 시간도 포함된다. 전송 오류 검사/정정을 할 수 있는 전송 단위

의 중간에 수신을 시작했을 때 해당 메시지는 무시할 수밖에 없다. 이것은 인증으로 인한 지연과는 상관이 없다. 이 척도는 유용한 메시지 단위를 수신하기 시작한 시점으로부터 인증 데이터 수신 대기를 위해 지연되는 최대 시간으로서 실질적인 지연시간이 될 것이다.

5.1.2 성능 비교

그림 10은 항법메시지에 대한 TFAF 예이다. 항법메시지 1번 서브프레임이 시작된 이후 수신을 시작할 경우 2번 서브프레임 수신이 완료되어야 인증할 수 있다. 유사한 방법으로 정밀보정 메시지에 대한 TFAF의 예는 그림 12와 같다. TBA는 인증 정보의 전송주기와 같으므로 항법메시지는 12초이고 정밀보정 메시지는 방법 1과 2에 대하여 각각 6초와 12초이다.

항법메시지에는 인증정보가 추가되지 않기 때문에 그로 인한 지연은 발생하지 않는다. 정밀보정 메시지에 대한 TFUD와 TBUD는 그림 12와 같으며, 실질적인 지연을 나타내는 DTFAF는 그림 13과 같이 방안 1, 2에 대하여 각각 5초와 11초이다. 각 성능 척도에 대한 분석값을 표 5에 정리하였다.

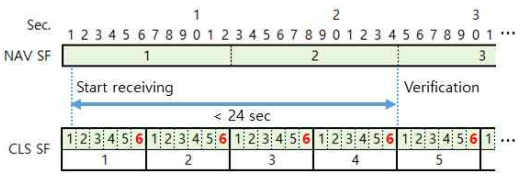

그림 10. 항법메시지에 대한 TFAF
Fig. 10. TFAF for NAV

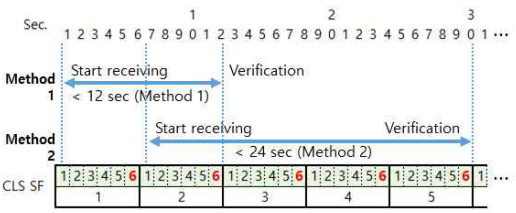

그림 11. 정밀보정 메시지에 대한 TFAF
Fig. 11. TFAF for CLS

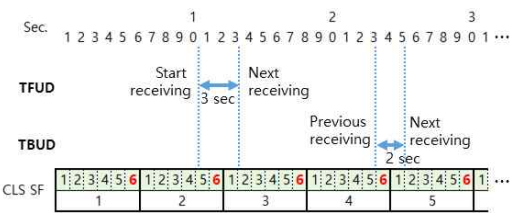

그림 12. 정밀보정 메시지에 대한 TFUD와 TBUD
Fig. 12. TFUD and TBUD for CLS

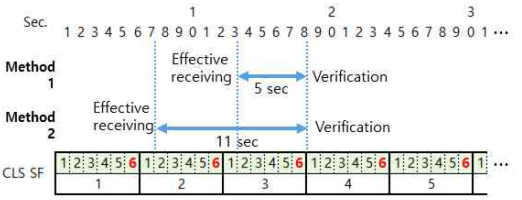

그림 13. 정밀보정 메시지에 대한 DTFAF
Fig. 13. DTFAF for CLS

표 5. 성능 비교
Table 5. Performance Comparison

Criteria	Target	Method 1	Method 2
TFAF	NAV	< 24	< 24
	CLS	< 12	< 24
TBA	NAV	12	12
	CLS	6	12
TFUD	NAV	< 24	< 24
	CLS	< 3	< 3
TBUD	NAV	< 12	< 12
	CLS	< 2	< 2
DTFAF	NAV	0	0
	CLS	< 5	< 11

5.2 안전성 분석

4.3.3절에서 기술한 바와 같이 안전성은 해시함수의 길이와 디지털 서명의 키길이에 의존한다. 한국인터넷진흥원에서 2030년 이전과 이후를 기준으로 권고하는 길이의 키를 사용할 수 있다. KPS는 2030년 이후에 발사될 예정이지만 위성의 낮은 성능을 고려하여 2030년까지의 권고사항인 112비트 보안강도를 가지는 224비트 길이의 키도 사용할 수 있으며, 2030년 이후의 권고사항인 128비트 보안강도 이상을 가지는 256, 384, 512비트 키도 사용할 수 있다. 단, Sig_{NAV}와 Sig_{CLS} 중 하나의 키 길이를 512비트로 사용할 경우, 다른 디지털 서명의 키길이는 384비트 이상 사용할 수 없다.

해시함수도 한국인터넷진흥원이 권고하는 해시 함수를 모두 선택하여 사용할 수 있다. 해시함수는 디지털 서명을 생성하기 전에 적용되어 전송량과는 무관하고 계산 속도도 디지털 서명에 비해 매우 빠르기 때문에 높은 강도를 가지는 해시함수를 적용하는 것이 바람직할 것이다.

Ⅵ. 결 론

GNSS 서비스가 다양한 영역으로 확대됨에 따라 정확도가 높은 위치정보가 요구된다. 또한 그에 대한 다양한 방법의 공격 시도도 증가할 것이며, 그로 인한

위협도 커질 것이다. 유럽의 Galileo를 시작으로 GPS, BeiDou, QZSS도 항법메시지에 대한 인증 서비스를 진행하고 있지만 정밀보정 서비스에 대한 인증 연구는 진행되고 있지 않다. 향후 다양한 서비스를 지원하게 될 KPS에서는 항법메시지 뿐만 아니라 정밀보정 서비스에 대한 인증서비스도 이루어져야 할 것이다.

본 논문에서는 KPS에 적용될 수 있도록 한국전자통신연구원에서 설계한 25bps 항법메시지와 일본에서 설계한 2000bps 정밀보정 메시지 구조를 이용하여 2가지 인증 방식 및 키관리 방식을 제안하였다. 제안 방식에서는 2030년 이후에도 한국인터넷진흥원에서 권고한 안전성을 제공할 수 있도록 다양한 보안 알고리즘과 키길이를 선택적으로 사용할 수 있다. 보안강도를 높일수록 전송량이 증가하므로 여러 가지 환경을 고려한 정책을 수립하여 적절하게 선택 적용할 수 있을 것으로 판단된다. 향후 우리나라의 정밀보정 메시지가 정의된다면 본 연구 결과를 적용한 인증기법을 설계할 수 있을 것으로 기대된다.

References

[1] S. Lee, et al., “Survey on navigation satellite system and technologies,” *ETRI Trends*, 2021.

[2] N. H. Kim and C. H. Park, “A study on the advanced altitude accuracy of GPS with barometric altitude sensor,” *J. IEEK*, vol. 49, no. 10, pp. 18-22, 2012.

[3] J. Zhang, X. Cui, H. Xu, and M. Lu, “A two-stage interference suppression scheme based on antenna array for GNSS jamming and spoofing,” *Sensors*, vol. 19, no. 18, 2019.

[4] European Commission, “*Tests of Galileo OSNMA underway*,” Feb. 2021, from https://ec.europa.eu/defence-industry-space/tests-galileo-osnma-underway-2021-02-11_en.

[5] A. Perrig, R. Canetti, J. D. Tygar, and D. Song, “The TESLA broadcast authentication protocol,” *RSA CryptoBytes*, vol. 5, no. 2, pp. 2-13, 2002.

[6] 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, Apr. 2019.

[7] Global Positioning Systems Directorate Systems Engineering & Integration, *NAVSTAR GPS Space Segment/UserSegment L1C Interface*, IS-GPS-800E, Apr. 2018.

[8] J. M. Anderson, et al., “Chips-message robust authentication (Chimera) for GPS civilian signals,” *ION GNSS+ 2017*, pp. 2388-2416, Sep. 2017.

[9] BeiDou Navigation Satellite System, *BeiDou Navigation Satellite System Signal In Space Interface Control Document Open Service Signal B2b v1.0*, Mar. 2020.

[10] Z. Wu, R. Liu, and H. Cao, “ECDSA-Based message authentication scheme for BeiDou-II navigation satellite system,” *Trans. Aerospace and Electr. Syst.*, vol. 55, no. 4, Aug. 2019.

[11] Z. Wu, Y. Zhang, and R. Liu, “BD-II NMA&SSI: An scheme of anti-spoofing and open BeiDou II D2 navigation message authentication,” *IEEE Access*, vol. 8, 2020.

[12] D. Manandhar and R. Shibasaki, “Authenticating GALILEO open signal using QZSS signal,” *ION GNSS+ 2018*, pp. 3995-4003, Miami, Florida, Sep. 2018.

[12] S. Lee, et al., “Prototyping of signal generator for satellite navigation payload,” *Electr. Telecommun.*, Jan. 2021.

[13] S. Lee, et al., “Navigation message and early warning service of RNSS,” in *Proc. KICS Conf. Commun.*, Jeju Island, Korea, Jun. 2021.

[14] T. Cho, et al., “Authentication for civil navigation message,” in *Proc. KICS Conf. Commun.*, Jeju Island, Korea, Jun. 2021.

[15] T. Cho, et al., “Authentication scheme for civil signals of navigation satellites,” *J. KICS*, vol. 46, no. 11, pp. 1882-1895, Nov. 2021.

[16] European GNSS Agency, *GALILEO HIGH ACCURACY SERVICE (HAS) info note*, 2020.

[17] Cabinet Office, *Quasi-Zenith Satellite System Interface Specification Centimeter Level Augmentation Service*, IS-QZSS-L6-004, Jul. 2021.

[18] China Satellite Navigation Office, *BeiDou Navigation Satellite System Signal In Space Interface Control Document Precise Point*

Positioning Service Signal PPP-B2b, 2019.
[19] NIST, *Advanced Encryption Standard, FIPS Publication 197*, 2001.
[20] H. J. Lee, et al., *The SEED Encryption Algorithm*, IETF RFC4269, 2005.
[21] R. L. Rivest, A. Shamir, and L. M. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Commun. ACM*, vol. 21, pp. 120-126, 1978.
[22] N. Koblitz, "Elliptic curve cryptosystems," *Math. Computation*, vol. 48, no. 177, pp. 203-209, 1987.
[23] NIST, *Secure Hash Standard, FIPS Publication 180-1*, Apr. 1995.
[24] NIST, *Secure Hash Standard, FIPS Publication 180-2*, Aug. 2002.
[25] D. Johnson, A. Menezes, and S. Vansto, "The elliptic curve digital signature algorithm (ECDSA)," *Int. J. Info. Secur.*, pp. 36-63, 2001.
[26] NIST, *Digital Signature Standard, FIPS Publication 186*, 1994.
[27] C. Lim and P. Lee, "The Korean certificate-based digital signature algorithm," *Comput. & Electr. Eng.*, vol. 25, pp. 249-265, 1999.
[28] KISA, *Guide for Crypto Algorithms and Key Length*, KISA, Dec. 2018.
[29] NIST, *NIST SP 800-57: Recommendation for Key Management: Part 1 – General*, NIST, May 2020.
[30] I. F. Hernández, et al., "Design drivers, solutions and robustness assessment of navigation message authentication for the galileo open service," *ION GNSS+ 2014*, pp. 2810-2827, Sep. 2014.

조 태 남 (Taenam Cho)

1986년 : 이화여자대학교 전자계산학과 졸업
1988년 : 이화여자대학교 전자계산학과 석사
2004년 : 이화여자대학교 컴퓨터학과 박사
1988년~1997년 : 한국전자통신연구원 위성관제연구실 선임연구원
2004년~2005년 : 이화여자대학교 컴퓨터학과 전임강사
2005년~2017년 : 우석대학교 정보보안학과 교수
2018년~현재 : 우석대학교 IT전자융합공학과 교수
<관심분야> 안드로이드 보안, IoT 보안, 위성보안
[ORCID:0000-0002-5191-0130]

용 승 림 (Seunglim Yong)

1996년 : 이화여자대학교 컴퓨터학과 졸업
1998년 : 이화여자대학교 컴퓨터학과 석사
2006년 : 이화여자대학교 컴퓨터학과 박사
2006년~2007년 : 이화여자대학교 컴퓨터학과 전임강사
2008년~현재 : 인하공업전문대학 컴퓨터시스템학과 교수
<관심분야> 컴퓨터보안, 위성보안
[ORCID:0000-0002-5903-303X]

정 원 찬 (Wonchan Jung)

1986년 12월 : Henderson State University 컴퓨터과학과 졸업
1992년 5월 : Louisiana State University 컴퓨터과학과 박사
1992년 6월~현재 : 한국전자통신연구원 근무
<관심분야> 인공위성 지상국 SW
[ORCID:0000-0001-6740-2643]

이 상 욱 (Sanguk Lee)

1988년 2월 : 연세대학교 천문기상학과 졸업
1991년 3월 : 미 Auburn대학교 항공우주공학 석사
1994년 3월 : Auburn대학교 항공우주공학 박사
1993년 3월~현재 : 한국전자통신연구원, 책임연구원, 현 KPS 위성항법연구센터 센터장
<관심분야> 위성항법, 항공우주공학, 이동통신공학
[ORCID:0000-0002-0744-5032]

유 준 규 (Ryu Joon Gyu)

1999년 2월 : 충남대학교 전파공학과 졸업
2001년 2월 : 충남대학교 전파공학과 석사
2014년 2월 : 충남대학교 전파공학과 박사
2001년 2월~현재 : 한국전자통신연구원 위성광역인프라연구실 실장
<관심분야> 위성통신, 시스템 엔지니어링
[ORCID:0000-0002-1449-4983]