JPNT 11(1), 1-9 (2022)
https://doi.org/10.11003/JPNT.2022.11.1.1

JPNT Journal of Positioning, Navigation, and Timing

Performance Analysis of Authentication Protocols of GPS, Galileo and BeiDou

Da-Yeon Jeon[1], Turabek Gaybullaev[1], Jae Hee Noh[2], Jung-Min Joo[3], Sang Jeong Lee[2], Mun-Kyu Lee[1†]

[1]Department of Electrical and Computer Engineering, Inha University, Incheon 22212, Korea
[2]Department of Electronics Engineering, Chungnam National University, Daejeon 34134, Korea
[3]GNSS R&D Division, Korea Aerospace Research Institute, Daejeon 34133, Korea

ABSTRACT

Global Navigation Satellite System (GNSS) provides location information using signals from multiple satellites. However, a spoofing attack that forges signals or retransmits delayed signals may cause errors in the location information. To prevent such attacks, authentication protocols considering the navigation message structure of each GNSS can be used. In this paper, we analyze the authentication protocols of Global Positioning System (GPS), Galileo, and BeiDou, and compare the performance of Navigation Message Authentication (NMA) of the above systems, using several performance indicators. According to our analysis, authentication protocols are similar in terms of performing NMA and using Elliptic Curve Digital Signature Algorithm (ECDSA). On the other hand, they are different in several ways, for example, whether to perform Spreading Code Authentication (SCA), whether to use digital certificates and whether to use Timed Efficient Stream Loss-tolerant Authentication (TESLA). According to our quantitative analysis, the authentication protocol of Galileo has the shortest time between authentications and time to first authenticated fix. We also show that the larger the sum of the navigation message bits and authentication bits, the more severely affected are the time between authentications and the time to first authenticated fix.

Keywords: authentication protocol, performance, GPS, Galileo, BeiDou

1. INTRODUCTION

다수의 인공위성으로부터 전송되는 신호의 시차를 분석하여 위치정보를 제공하는 위성항법시스템은, 군사 분야 및 교통, 항공, 농업 등 다양한 산업 분야에 널리 활용되고 있다 (Caparra et al. 2016, Margaria et al. 2017). 위성항법시스템 중 전세계를 대상으로 서비스를 제공하는 Global Navigation Satellite System (GNSS)으로 유럽의 Galileo (European Commission 2018, European Union Agency for the Space Programme 2021), 미국의 Global Positioning System (GPS) (Air Force Research Laboratory Space Vehicles Directorate Advanced GPS Technology 2019), 중국의 BeiDou (China Satellite Navigation Office 2019), 러시아의 Global Navigation Satellite System (GLONASS) (Russian Space Systems OJSC 2016) 등이 운용되고 있다. 그러나 공격자가 위성에서 전송된 신호를 변조하거나 신호를 저장한 후 시간차를 두고 재 전송함으로써 위치 정보에 오류를 발생시키는 공격(기만 공격)이 가능하므로, 이와 같은 공격을 방지하기 위한 신호 인증이 필요하다 (Margaria et al. 2017). 신호 인증은 여러 암호 알고리즘들을 이용하여 위성 신호의 위조 여부를 확인할 수 있는 방법이다. 대표적인 GNSS 신호 인증 방법으로 GPS의 Chips Message Robust Authentication (Chimera) (Air Force Research Laboratory Space Vehicles Directorate Advanced GPS Technology 2019)와 Galileo의 Open Service Navigation Message Authentication (OSNMA) (European Commission 2018, European Union Agency for the Space Programme 2021)이 있다. 이 외에도 BeiDou에 대해서는

Received Jan 01, 2022 **Revised** Jan 17, 2022 **Accepted** Feb 08, 2022
†**Corresponding Author**
E-mail: mklee@inha.ac.kr
Tel: +82-32-860-7456 Fax: +82-32-873-7456
Da-Yeon Jeon https://orcid.org/0000-0003-1645-1570
Turabek Gaybullaev https://orcid.org/0000-0003-2768-4898
Jae Hee Noh https://orcid.org/0000-0002-6314-738X
Jung-Min Joo https://orcid.org/0000-0002-8256-7005
Sang Jeong Lee https://orcid.org/0000-0002-9400-5157
Mun-Kyu Lee https://orcid.org/0000-0003-4423-7467

Chimera, OSNMA와 같이 공식 문서는 없지만, 인증 프로토콜로 제안된 두 가지 방법이 있다 (Wu et al. 2019, 2020).

Margaria et al. (2017)는 GNSS에서 발생할 수 있는 위험과 GNSS의 인증 프로토콜의 기능을 포함하여 GNSS와 관련된 동향을 서술하였다. Air Force Research Laboratory Space Vehicles Directorate Advanced GPS Technology (2019)는 Chimera의 Interface Control Document (ICD)로 항법 메시지 구조와 암호 알고리즘을 서술하였고, Gamba et al. (2020)는 Chimera의 구조를 그림과 함께 설명하였다. OSNMA의 전체 구조는 OSNMA의 ICD인 European Commission (2018)에 정리되어 있다. BeiDou의 인증 프로토콜로 Wu et al. (2019)는 ECDSA (National Institute of Standards and Technology 2013) 기반 방법을 제안하였고, Wu et al. (2020)는 Timed Efficient Stream Loss-Tolerant Authentication (TESLA) (Perrig et al. 2000) 기반 방법을 제안하였다. Wu et al. (2020)는 중국의 해시 표준 함수인 SM3 (Standardization Administration of the People's Republic of China 2016)와 타원곡선 기반의 전자서명인 SM2 (China's State Cryptography Administration 2010)를 사용하였다. Jeon et al. (2021a)는 GPS와 Galileo의 항법 메시지 구조와 인증 프로토콜 구조를 비교 분석하였고, Gaybullaev et al. (2021)는 GPS와 Galileo의 인증 프로토콜 비교 시, 여러 성능 지표를 사용하여 성능을 비교하였다. 마지막으로 Jeon et al. (2021b)는 Jeon et al. (2021a)에서 BeiDou를 분석 대상에 추가하여 GPS, Galileo와 BeiDou의 항법 메시지가 가진 특징과 인증 프로토콜의 구조를 비교하고 각 인증 프로토콜의 공통점과 차이점을 분석하였다.

본 논문에서는 GPS, Galileo와 BeiDou의 항법 메시지와 인증 프로토콜의 구조를 비교하고 여러 성능 지표를 통해 인증 프로토콜들의 성능을 비교 분석한다. 본 논문은 Jeon et al. (2021b)의 확장판으로, 인증 프로토콜의 구조에 대한 자세한 설명과 인증 프로토콜들의 성능을 비교한 정량 분석을 추가하였다. 인증 프로토콜의 주요 정량 성능 지표로 인증 간 시간 및 최초 인증까지의 시간을 고려하였으며, 이 지표에 대한 비교를 통해 일반적인 환경에서 OSNMA의 성능이 가장 좋으며 D1 기반 BeiDou-ECDSA의 성능이 가장 좋지 않음을 확인하였다. 한편 Chimera는 항법메시지의 길이가 길기 때문에, 비트 에러율 증가에 따른 인증 간 시간 및 최초 인증까지의 시간에 대한 증가율이 크다는 사실도 확인하였다.

본 논문의 구성은 다음과 같다. 2장은 GPS, Galileo와 BeiDou의 항법 메시지를 비교한 후, 해당 GNSS의 인증 프로토콜을 분석한다. 3장은 2장에서 제시된 인증 프로토콜들을 사용하는 암호 알고리즘에 따라 정성적으로 비교하고, 여러 성능 지표에 따라 인증 프로토콜들의 성능을 정량적으로 비교한다. 마지막 4장은 결론으로, 본 논문에서 다룬 비교 분석 결과를 정리하고 한계점 및 향후 계획을 제시하였다.

2. AUTHENTICATION PROTOCOLS

2.1 Navigation Message

본 논문에서 분석하는 GNSS는 GPS, Galileo와 BeiDou이다.

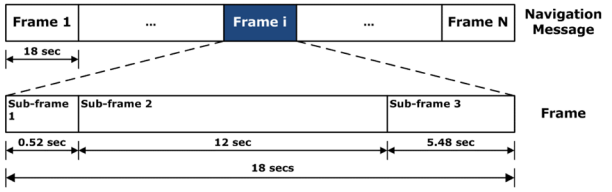


Fig. 1. GPS navigation message structure (ESA NAVIPEDIA – GPS navigation message 2011).

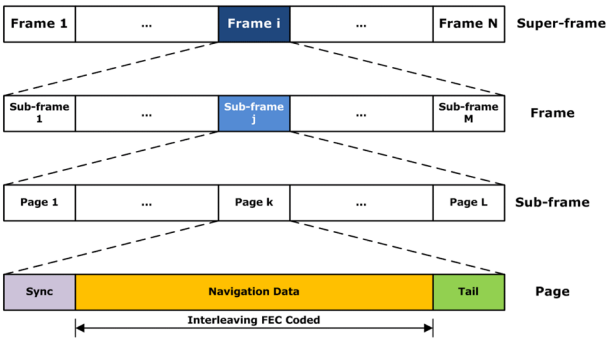


Fig. 2. Galileo navigation message structure (ESA NAVIPEDIA – Galileo navigation message 2011).

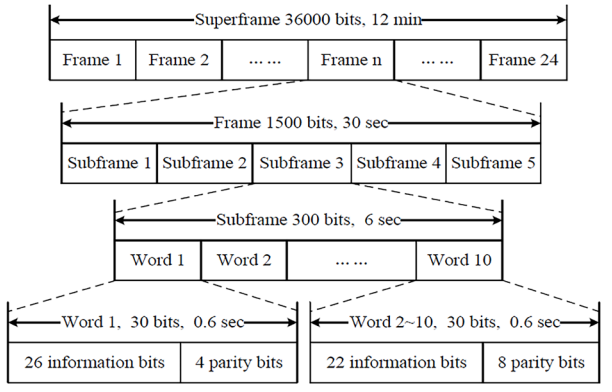


Fig. 3. BeiDou D1 navigation message (China Satellite Navigation Office 2019).

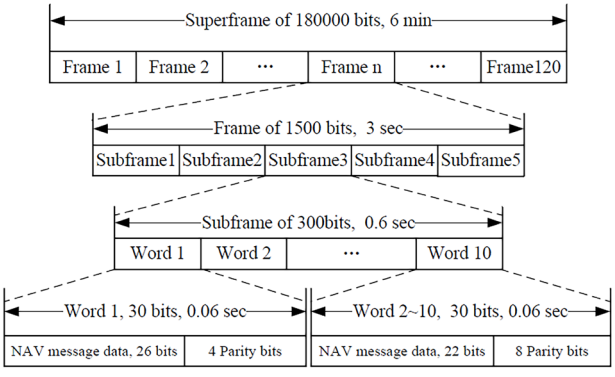


Fig. 4. BeiDou D2 navigation message (China Satellite Navigation Office 2019).

Table 1. Summary table for navigation messages.

	GPS	Galileo	BeiDou	
Name of navigation message	CNAV-2	Galileo I/NAV	D1	D2
Duration of frame (sec)	180	720	30	3
Size of navigation message (bits)	9,000	90,000	1,500	1,500
Number of subframe	3	24	5	5
Structure of subframe	10 pages	15 pages	10 words	10 words
Transmission rate (bps)	50	125	50	500

GPS의 인증 프로토콜에서 사용하는 항법 메시지는 CNAV-2 navigation message이고 Galileo의 인증 프로토콜에서 사용하는 항법 메시지는 Galileo I/NAV navigation message이다. BeiDou는 BeiDou D1 navigation message와 BeiDou D2 navigation message (China Satellite Navigation Office 2019)를 항법 메시지로 사용한다. 각 항법 메시지의 구조는 GPS, Galileo, BeiDou 순으로 Figs. 1-4와 같다. Jeon et al. (2021b)에서 항법 메시지의 특징을 Table 1에 정리하였다. 항법 메시지는 frame의 지속 시간, 항법 메시지의 크기, subframe의 개수와 구조, 전송률을 기준으로 비교할 수 있다. Bps 단위를 사용하는 전송률은 항법 메시지 크기를 frame의 지속 시간으로 나누면 된다. Table 1에 따르면, BeiDou의 D2 Navigation message의 frame 지속 시간이 가장 짧고 전송률이 500 bps로 가장 높음을 확인할 수 있다.

2.2 Chimera

Chimera는 Navigation Message Authentication (NMA), Spreading Code Authentication (SCA) 두 종류의 기능을 수행하고 전체 구조는 Fig. 5와 같다. NMA는 GPS CNAV-2 navigation message를 입력으로 하여 전자서명을 생성하고 검증한다. 전자서명 알고리즘으로 224 비트 타원곡선 기반의 ECDSA P-224가 사용되고 그 결과로 448 비트의 전자서명이 생성된다. SCA를 위한 marker를 생성하기 위해 marker key가 필요하고 marker key의 종류로는 fast channel marker key와 slow channel marker key가 있다. Fast channel marker key는 Fast Channel 주기의 시작 시간을 입력으로 사용하고 HMAC-SHA-256을 암호 알고리즘으로 사용하여 256 비트의 key를 생성한다. 반면에, Slow channel marker key는 NMA의 결과로 나온 448 비트의 전자서명을 입력으로 사용하고 SHA-512/256을 암호 알고리즘으로 사용하여 256 비트의 key를 생성한다. 마지막으로 생성된 fast channel marker key와 slow channel marker key를 사용하여 SCA에 해당하는 marker value와 marker location이 생성된다. Marker value와 Marker location은 128 비트이고 fast channel marker key 또는 slow channel marker key를 AES-256의 key로 사용한다. AES-256으로 생성된 marker value ciphertext와 marker location ciphertext는 Message Authentication Codes (MAC) 역할을 하게 되어 SCA를 수행한다.

2.3 OSNMA

OSNMA는 이름과 같이 NMA만을 수행하며, 공개키 검증, TESLA (Perrig et al. 2000) root key 검증, TESLA key chain 생성 및 TESLA key 검증, MAC 검증 순서로 진행된다. OSNMA의 구조는 Fig. 6과 같다.

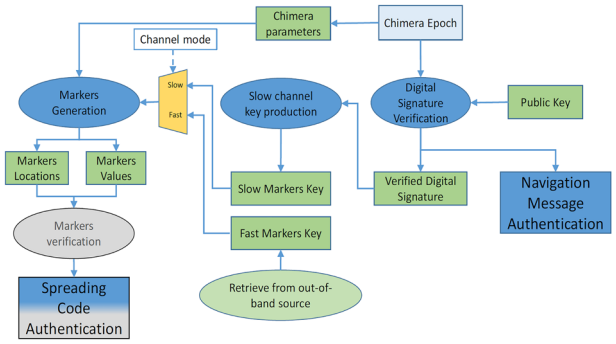


Fig. 5. Block diagram of the Chimera (Gamba et al. 2020).

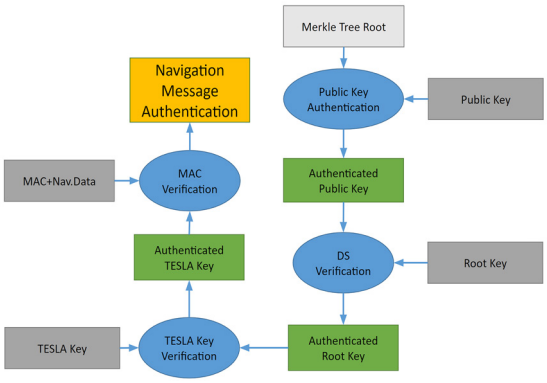


Fig. 6. Block diagram of the OSNMA.

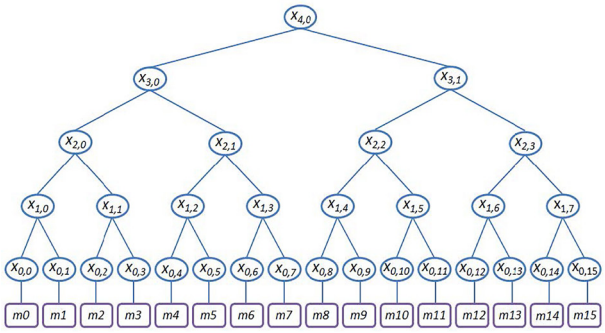


Fig. 7. Merkle tree with N=16 elements (European Commission 2018).

OSNMA에서는 공개키의 갱신시 새로운 키의 검증을 위해 높이가 4이고 leaf 노드가 16개로 구성된 Merkle tree를 사용하는데, 그 구조는 Fig. 7과 같다. 각 leaf 노드는 미리 정해져 있는 16개의 공개키로, m_0부터 m_{15}로 나타내기로 한다. 수신기는 이미 보유하고 있는 root hash($x_{4,0}$)와 위성으로부터 전송받은 중간 해시값들을 입력으로 leaf로부터 root까지 식 (2)와 같이 해시함수 f를 계산함으로써 공개키를 검증한다. 예를 들어 현재 사용하는 키가 m_4이고, 이를 m_5로 갱신하는 상황이라면, 먼저 검증 대상 키인 m_5에 식 (1)을 적용하여 $x_{0,5}$를 계산하고, 위성에서 전송된 $x_{0,4}$, $x_{1,3}$, $x_{2,0}$, $x_{3,1}$을 식 (2)에 대입하여 $x_{1,2}$, $x_{2,1}$, $x_{3,0}$, $x_{4,0}$을 차례로 계산한다.

계산의 최종 결과인 $x_{4,0}$가 수신기가 이미 보유한 $x_{4,0}$과 같다면 검증에 성공하고, 키를 m_5로 성공적으로 갱신하게 된다. 함수 f로 사용하는 해시 알고리즘은 SHA-256이다.

$$x_{0,i} = f(m_i); i = 0, \ldots 15 \tag{1}$$

$$x_{j,i} = f\left(x_{j-1;2i} || x_{j-1;2i+1}\right) \tag{2}$$

다음은 전자서명을 통한 root key 검증에 대해 설명한다. OSNMA는 ECDSA P-224, ECDSA P-256, ECDSA P-384, 또는 ECDSA P-521등 다양한 전자서명을 사용 가능하나, 본 논문은 가장 전형적인 파라미터인 ECDSA P-256 전자서명을 예로 설명한다. 위와 같이 검증된 공개키를 이용하면 전자서명의 검증이 가능한데, 검증의 대상은 실제 항법 메시지 인증에 사용되는 TESLA key chain의 root key에 대한 서명이다. TESLA key chain은 현재의 TESLA key에 SHA-256, SHA3-224 또는 SHA3-256 해시 함수를 적용하여 새로운 TESLA key를 도출하는 일을 연쇄적으로 수행함으로써 생성되며, 본 논문에서는 SHA-256 해시 함수를 사용한 경우를 분석하였다. 이를 일정 횟수 반복한 최종 TESLA key가 root key로 전자서명의 대상이 된다. 그러나 TESLA key를 MAC 기반의 인증에 사용할 때는 생성된 순서의 역순으로, 즉 root key부터 사용하게 된다. 따라서 데이터의 인증을 수행하기 전에, TESLA key의 해시 값이 이전 TESLA key와 같은지 확인함으로써 현재의 TESLA key를 검증하게 된다. 인증의 마지막 단계는 MAC & Key (MACK) 블록들의 MAC을 생성하고 검증하는 것으로서, 다음 메시지 블록에 포함된 TESLA key를 이용하여 MAC을 통해 검증된다.

2.4 TESLA Based BeiDou Authentication Proposal

Wu et al. (2020)에서는 OSNMA에서도 사용된 TESLA를 기반으로 하는 BeiDou의 인증 프로토콜을 제안하였다. 그 전체 구조는 Fig. 8과 같다. 본 논문에서는 이 방법을 BeiDou-TESLA라 칭한다. BeiDou-TESLA에서 사용하는 항법 메시지는 BeiDou D2 navigation message이고 OSNMA와 달리 중국의 표준 해시 함수인 SM3 (Standardization Administration of the People's Republic of China 2016)를 사용한다. Wu et al. (2020)에 의하면, Certification Authority (CA)는 인증에 사용할 다양한 키를 생성하고 키 중에서 공개키는 TESLA의 root key 인증에 사용된다. BeiDou-TESLA에서는 SM3를 사용하여 TESLA key chain을 생성하며, 중국의 타원곡선 기반의 전자서명인 SM2 (China's State Cryptography Administration 2010)로 검증된 root key를 이용하여 TESLA key chain을 검증한다. BeiDou-TESLA에서 key chain 생성에 사용하는 식은 식 (3-4)와 같다. 식 (3)에서 K_i는 i번째 key를 의미하고 BDT_j는 subframe j의 위성 시간 인증 타임스탬프를 의미한다. 식 (4)에서 SM3로 256 비트의 키를 생성하고 길이가 128 비트가 되도록 cut 함수를 사용한다.

$$K_{i-1} = F(K_i, BDT_j) \tag{3}$$

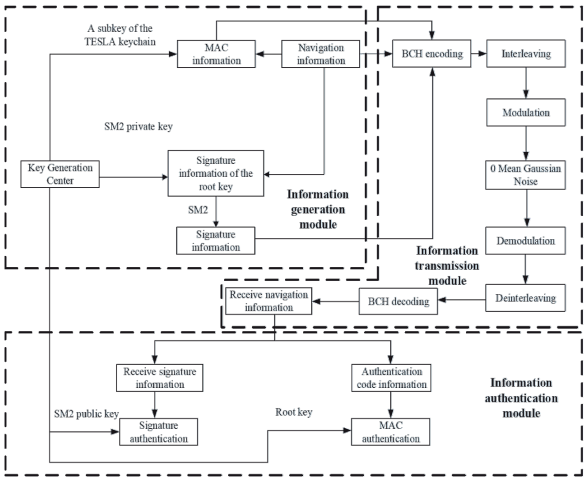


Fig. 8. Block diagram of the BeiDou-TESLA (Wu et al. 2020).

$$F\left(K_i, BDT_j\right) = cut(len, SM3(K_i || BDT_j) \tag{4}$$

2.5 ECDSA Based BeiDou Authentication Proposal

ECDSA 기반의 BeiDou 인증 프로토콜은 Wu et al. (2019)에서 제안한 방법으로 본 논문에서는 이를 BeiDou-ECDSA라 칭한다. BeiDou-ECDSA는 BeiDou의 D1과 D2 navigation message를 모두 사용하고 128 비트 타원곡선 기반의 ECDSA를 사용한다. 이 프로토콜의 ECDSA에서 사용하는 공개키는 인터넷에서 가져온 디지털 인증서를 통해 추출할 수 있다. Figs. 9와 10은 D1과 D2 navigation message에 대한 BeiDou-ECDSA의 전체 구조이다.

D1 기반 BeiDou-ECDSA의 경우, main-frame 11의 subframe 1~3 중 547 비트의 basic navigation data가 ECDSA P-128의 입력으로 사용되고, 서명의 결과로 304 비트가 page 11의 subframe 5의 51~228 비트와 page 12의 subframe 5의 51~176 비트에 저장된다. 또한 동일한 서명의 결과가 page 23의 subframe 5의 51~228 비트와 page 24의 subframe 5의 51~176 비트에도 저장된다. D2 기반 BeiDou-ECDSA의 경우에는 ECDSA의 입력으로 main-frame 1~10의 subframe 1 중 547 비트의 basic navigation data를 사용하고 서명의 결과는 page 1의 subframe 1의 151~262 비트, page 2의 subframe 1의 151~262 비트와 page 3의 subframe 1의 151~230 비트에 총 304 비트가 저장된다. 이는 Distinguished Encoding Rules를 사용하여 서명 결과의 필요 비트 수가 다소 증가한 것으로 파악된다. 입력으로 사용된 항법 메시지에 SHA-256을 적용한 결과와 공개키를 이용하여 서명 검증이 수행된다.

3. PERFORMANCE COMPARISON

3.1 Comparison of Authentication Protocols

네 종류의 인증 프로토콜은 모두 공통적으로 NMA를 수행하고 전자서명을 사용한다. Chimera, OSNMA와 BeiDou-ECDSA는 국제 표준 ECDSA를 사용하고 BeiDou-TESLA는 중국의 타

Table 2. Summary table for authentication protocols.

	Chimera	OSNMA	BeiDou-TESLA	BeiDou-ECDSA
NMA	O	O	O	O
SCA	O	X	X	X
Elliptic curve based digital signature	ECDSA	ECDSA	SM2	ECDSA
Digital certificate	X	X	O	O
TESLA	X	O	O	X
Function for generating TESLA key chain	-	SHA-256	SM3	-

원곡선 전자서명 표준인 SM2를 사용한다는 차이점이 있지만 모든 인증 프로토콜에서 타원곡선 기반의 전자서명을 사용하고 있다. Chimera는 다른 인증 프로토콜들과 달리 SCA를 추가로 수행하기 위해 marker라는 개념이 사용된다. OSNMA와 BeiDou-TESLA는 공통적으로 TESLA를 사용하지만, TESLA의 세부 구조를 분석하면 OSNMA는 Secure Hash Algorithm을 사용하여 key chain을 생성하는 반면에, BeiDou-TESLA는 중국의 해시 표준인 SM3를 사용한다. 또한, OSNMA는 Merkle tree로 검증된 공개키를 사용하는 반면에, BeiDou의 인증 프로토콜 두 방법에서는 인증서로부터 추출된 공개키를 사용한다. BeiDou의 인증 프로토콜로 제안된 두 가지 방법은 모두 인증서를 사용한다는 점에서 Chimera, OSNMA와 차이점을 가진다. 인증 프로토콜의 공통점과 차이점을 간단하게 Table 2와 같이 정리하였다.

3.2 Performance Indicators

본 논문에서는 인증 프로토콜의 성능 비교를 위한 주요 지표로 Fernández-Hernández et al. (2014)에서 사용된 Time Between Authentications (TBA) 및 Time To First Authenticated Fix (TTFAF)를 사용한다. 이들 지표를 도출하기 위해 NNA, Bit Error Rate (BER), Authentication Error Rate (AER) 등의 파라미터들이 사용된다. 여기서 NNA는 navigation message의 비트 수 (NN)와 해당 navigation message에 대한 인증 비트 수 (NA)의 합을 의미한다. BER은 비트의 오류 확률이고 AER은 공격이 없을 때 인증 받는 위성에서 오류가 생길 수 있는 확률을 의미한다. 식 (5)는 AER과 BER, NNA의 관계를 나타낸다.

$$\mathrm{AER}=1-(1-BER)^{NNA} \tag{5}$$

한편 TBA는 하나의 위성에 대한 연속적인 두 개의 인증 사이의 시간을 의미한다. 한편, OSNMA에서는 TESLA key chain이 모두 소모되어 새로운 전자서명의 전송과 확인이 필요할 때, 수신자가 새로운 root key와 이에 대한 전자서명을 기다려야 하는 상황이 발생한다. Gaybullaev et al. (2021)에서는 이러한 경우를 Cold start라 하고 이 상황에서의 성능을 비교하기 위해 TBA의 변형된 형태로 Time Between Signatures (TBS)라는 추가적인 성능 지표를 정의하였다. TTFAF는 처음 인증이 완료될 때까지의 시간을 의미한다. TBA와 TBS는 항법 메시지 구조 및 전송률이 결정되면 간단히 계산되는 값이지만, 실제 항법 메시지가 전송되는 환경에서는 오류로 인해 재전송이 필요할 수 있으므로 실제로는 더 긴 시간이 필요하게 된다. 이렇게 오류의 영향을 고려한 TBA의 기대값과 TBS의 기대값을 각각 $\overline{TBA}$, $\overline{TBS}$라 정의하는데, 이들은 식 (6)과 (7)에 의해 계산될 수 있다. TTFAF의 기대값인 $\overline{TTFAF}$도 역시 비슷한 방법으로 계산이 가능하나, hot start 상황의 $\overline{TTFAF}$는 TBA를 이용하여 계산되며, cold start 상황의 $\overline{TTFAF}$는 TBS를 이용하여 계산된다. 이 두 상황에서의 $\overline{TTFAF}$ 계산식은 각각 식 (8), (9)와 같다. 여기서 TBA/2 및 TBS/2 항들은 이미 인증 메시지가 전송되고 있는 상황에서 다음 인증 세션의 시작을 기다리기 위한 평균 시간을 반영한 것이다.

Table 3. Base values for Chimera, OSNMA, BeiDou-TESLA, BeiDou-ECDSA.

	NN	NA	NNA	TBA	TBS
Chimera	7902	448	8350	180	180
OSNMA	600	156	756	10	-
OSNMA (cold)	832	668	1500	-	240
BeiDou-TESLA	557	1500	2057	15	15
BeiDou-ECDSA (D1)	547	304	851	360	360
BeiDou-ECDSA (D2)	547	304	851	30	30

$$\overline{TBA}=\frac{TBA}{1-AER} \tag{6}$$

$$\overline{TBS}=\frac{TBS}{1-AER} \tag{7}$$

$$\overline{TTFAF}=\frac{TBA}{2}+\overline{TBA} \tag{8}$$

$$\overline{TTFAF}(cold\ start)=\frac{TBS}{2}+\overline{TBS} \tag{9}$$

3.3 Performance Comparison of Authentication Protocols

이번 절에서는 앞에서 설명한 네 가지 인증 프로토콜의 NMA 성능을 3.2절에서의 성능 지표를 사용하여 비교한다. 먼저 Table 3은 성능 비교를 위한 기초 파라미터인 NN, NA, NNA와, 기본적인 성능 지표인 TBA, TBS를 정리하여 보여주고 있다. 먼저 Chimera는 835 비트의 frame 10개로 구성되므로 NNA는 8350 비트이다. 각 frame은 9 비트의 subframe 1, 576 비트의 subframe 2와 250 비트의 subframe 3으로 구성되어 있는데, Page 8의 subframe 3 중 212 비트와 Page 9의 subframe 3 중 236 비트가 인증을 위해 사용되므로 NA는 448 비트이고, NN은 8350 비트의 NNA에서 448 비트의 NA를 뺀 값인 7902 비트이다.

OSNMA는 TBA와 TBS를 각각 고려해야 하고 해당 상황에 따른 NNA가 다르게 나온다. 전자서명이 이미 확인되어 TESLA의 MAC 연산만 수행되는 hot start 경우에는 3개의 MACK 블록에 전송된 MAC이 10초마다 검증되므로 TBA는 10초이다. NN은 8 비트의 PRN_A, 32 비트의 Galileo System Time, 8 비트의 counter, 2 비트의 NMA Status, 549 비트의 navdata와 1 비트의 padding의 합인 600 비트이고 NA는 128 비트의 TESLA key, 12 비트의 MAC tag와 16 비트의 MAC info의 합인 156 비트이다. 따라서 OSNMA의 hot start의 NNA는 756 비트이다. 반면에, cold start인 경우, 전자서명의 입력으로 사용되는 8 비트의 header, 96 비트의 DSM0 block과 128 비트의 Root key가 NN으로 추가되어야 하고 NA는 ECDSA P-256의 결과인 512 비트의 전자서명이 추가되어야 한다. 따라서, cold start의 NN은 832 비트이고 NA는

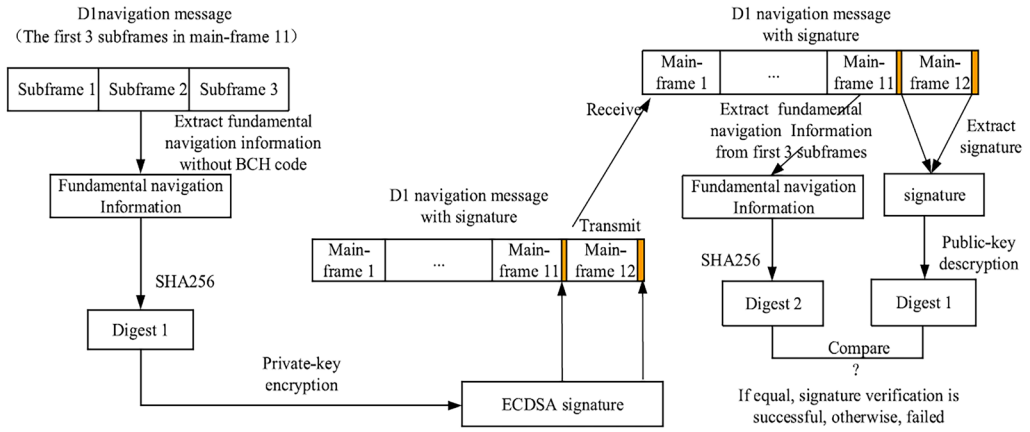


Fig. 9. Block diagram of the BeiDou-ECDSA based on D1 navigation message (Wu et al. 2019).

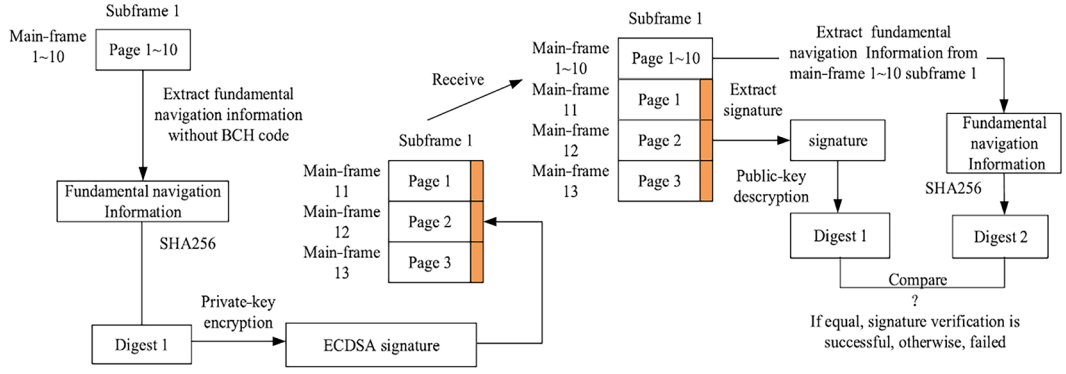


Fig. 10. Block diagram of the BeiDou-ECDSA based on D2 navigation message (Wu et al. 2019).

668 비트, NNA는 1500 비트이고 TBS는 240초이다.

BeiDou-TESLA의 NN은 Ephemeris and clock offset parameters, Satellite Autonomous Health Information Identification, Ionospheric delay correction model parameters와 User Range Accuracy index를 포함하는 557 비트이다. BeiDou-TESLA도 OSNMA와 같이 전자서명과 TESLA MAC을 별도로 고려하여야 하지만, BeiDou-TESLA의 root key는 디지털 인증서에 포함되어 있으므로 cold start를 따로 고려하지 않아도 된다. 따라서 NA는 서명이 수신될 때마다 검증된 비트를 포함하고 NN과 같이 처음 5 pages와 마지막 5 pages에 똑같이 나눠서 받지 않고 2개의 MAC을 한번에 받게 되어 총 1500 비트가 된다. NN과 NA를 합하면, NNA는 2057 비트가 되고 TBA는 15초이다.

BeiDou-ECDSA에서 D1 navigation message를 사용하는 경우, Fig. 9에 따르면, main-frame 11에서 300 비트의 subframe 3개 중 547 비트의 basic navigation data가 NN에 해당되고 ECDSA의 결과로 저장되는 304 비트가 NA이므로 NNA는 851 비트이다. 이 경우의 TBA는 D1 navigation message의 page 11과 12, page 23과 24에 동일한 서명이 삽입되므로 360초이다. BeiDou-ECDSA에서 D2 navigation message를 사용하는 경우, Fig. 10에 따르면, main-frame 1~10에서 각 300 비트의 subframe 1중 547 비트의 basic navigation data가 NN에 해당되고 D1 navigation message와 달리 304 비트의 전자서명 결과만을 사용하므로 NA는 304 비트이다. 그러므로 NNA는 851 비트이고 10개의 연속적인 mainframe이 30초 동안 전송되므로 TBA는 30초가 된다.

Table 4. AER according to BER.

	10^{-8}	10^{-7}	10^{-6}	10^{-5}	10^{-4}
Chimera	0.0000835	0.0008347	0.0083152	0.0801093	0.5661436
OSNMA	0.0000076	0.0000756	0.0007557	0.0075315	0.0728165
OSNMA (cold)	0.0000150	0.0001500	0.0014989	0.0148881	0.1392985
BeiDou-TESLA	0.0000206	0.0002057	0.0020549	0.0203600	0.1859311
BeiDou-ECDSA (D1)	0.0000085	0.0000851	0.0008506	0.0084739	0.0815835
BeiDou-ECDSA (D2)	0.0000085	0.0000851	0.0008506	0.0084739	0.0815835

Table 4는 BER의 변화에 따른 AER을 보여준다. 표에 따르면, 같은 BER에 대해 Chimera의 AER이 가장 크고 OSNMA의 AER이 가장 작음을 확인할 수 있다. 이는 식 (5)에 따라 NNA가 클수록 AER이 커지기 때문이다. 또한, NNA가 같은 D1 기반 BeiDou-ECDSA와 D2 기반 BeiDou-ECDSA의 BER에 따른 AER은 동일하다.

Table 5는 위의 AER로 식 (6)의 $\overline{TBA}$와 식 (7)의 $\overline{TBS}$를 계산하여 정리한 표이며, Fig. 11은 이를 그래프로 나타낸 것이다. 식 (6-7)에 따르면, $\overline{TBA}$와 $\overline{TBS}$는 AER이 클수록 커지고 AER이 작을수록 작아진다. Table 5를 통해 NNA 및 TBA의 값이 작은

Table 5. $\overline{TBA}$ and $\overline{TBS}$ according to BER.

	10^{-8}	10^{-7}	10^{-6}	10^{-5}	10^{-4}
Chimera $\overline{TBA}$	180.0150	180.1504	181.5093	195.6754	414.8839
OSNMA $\overline{TBA}$	10.0001	10.0008	10.0076	10.0759	10.7854
OSNMA (cold) $\overline{TBS}$	240.0036	240.0360	240.3603	243.6272	278.8423
BeiDou-TESLA $\overline{TBA}$	15.0003	15.0031	15.0309	15.3117	18.4260
BeiDou-ECDSA (D1) $\overline{TBA}$	360.0031	360.0306	360.3065	363.0767	391.9790
BeiDou-ECDSA (D2) $\overline{TBA}$	30.0003	30.0026	30.0255	30.2564	32.6649

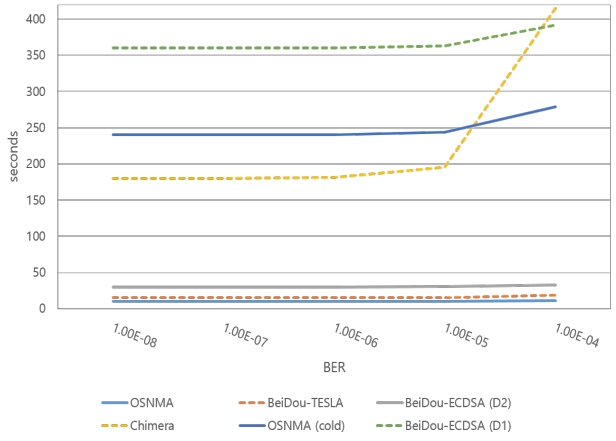


Fig. 11. Estimated $\overline{TBA}$ and $\overline{TBS}$ according to BER.

Table 6. $\overline{TTFAF}$ according to BER.

	10^{-8}	10^{-7}	10^{-6}	10^{-5}	10^{-4}
Chimera	270.0150	270.1504	271.5093	285.6754	504.8839
OSNMA	15.0001	15.0008	15.0076	15.0759	15.7854
OSNMA (cold)	360.0036	360.0360	360.3603	363.6272	398.8423
BeiDou-TESLA	22.5003	22.5031	22.5309	22.8117	25.9260
BeiDou-ECDSA (D1)	540.0031	540.0306	540.3065	543.0767	571.9790
BeiDou-ECDSA (D2)	45.0003	45.0026	45.0255	45.2564	47.6649

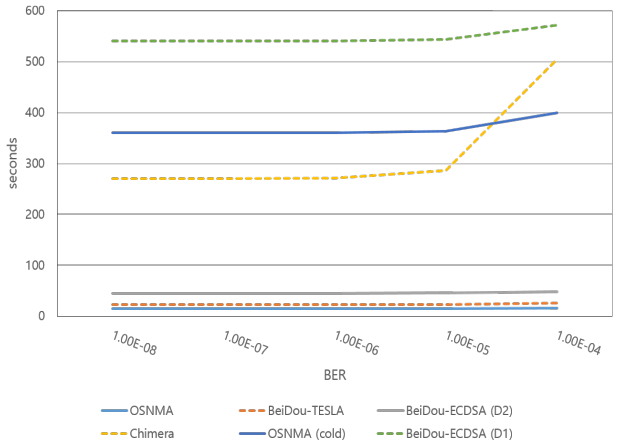


Fig. 12. Estimated $\overline{TTFAF}$ according to BER.

OSNMA, BeiDou-TESLA, D2 기반 BeiDou-ECDSA 순으로 $\overline{TBA}$가 짧게 걸림을 확인할 수 있다. 반면에, TBA가 가장 긴 D1 기반의 BeiDou-ECDSA인 경우, $\overline{TBA}$가 10^{-4}보다 작은 경우에 가장 긴 것을 확인할 수 있다. 한편, NNA가 가장 긴 Chimera는 BER이 커짐에 따라 AER이 급격히 커지므로 $\overline{TBA}$의 변화율이 큰 것을 Fig. 11로 확인할 수 있다. BER이 10^{-5}보다 작은 경우, $\overline{TBS}$가 큰 OSNMA (cold start)의 $\overline{TBS}$가 Chimera의 $\overline{TBA}$보다 크지만, BER이 10^{-5}보다 큰 경우, NNA가 다른 인증 프로토콜보다 월등히 큰 Chimera의 소요 시간이 길다. 이를 통해 NNA가 긴 인증 프로토콜은 BER이 커질수록 $\overline{TBA}$의 변화 추이가 커짐을 알 수 있고 $\overline{TBA}$ 또는 $\overline{TBS}$가 짧아야 BER에 따른 $\overline{TBA}$ 또는 $\overline{TBS}$의 소요 시간이 짧아서 유리한 면을 가진다고 할 수 있다.

Table 6 및 Fig. 12는 BER에 따른 $\overline{TTFAF}$의 변화를 보여주고 있는데, $\overline{TBA}$ 및 $\overline{TBS}$와 유사한 경향을 확인할 수 있다. $\overline{TBA}$가 작은 것부터 OSNMA, BeiDou-TESLA, D2 기반 BeiDou-ECDSA를 보면, $\overline{TTFAF}$의 순서도 동일함을 확인할 수 있다. 또한, Table 5와 마찬가지로 D1 기반 BeiDou-ECDSA의 $\overline{TTFAF}$가 가장 길지만 변화율은 크지 않은 반면에, D1 기반 BeiDou-ECDSA에 비해 TBA가 절반, 즉 180초인 Chimera는 BER이 커짐에 따라 $\overline{TTFAF}$가 D1 기반 BeiDou-ECDSA의 그것에 거의 근접함을 확인할 수 있다. 또한, NNA가 큰 Chimera는 BER이 10^{-5}보다 작은 경우에는 $\overline{TBA}$와 $\overline{TTFAF}$의 변화율이 크지 않지만, BER이 1에 가까워질수록 두 지표의 변화율이 급격히 커진다. 이는 OSNMA (cold start)와 Chimera의 결과 비교를 통해 확인할 수 있다. 위 결과를 요약하면, TBA 또는 TBS가 클수록 $\overline{TBA}$, $\overline{TBS}$와 $\overline{TTFAF}$가 길지만, NNA가 클 경우는 BER의 증가에 따른 $\overline{TBA}$, $\overline{TBS}$와 $\overline{TTFAF}$의 증가 속도가 급격히 커짐을 알 수 있다.

4. CONCLUSIONS

이 논문에서는 GPS, Galileo, BeiDou 등 세 종류의 GNSS를 위한 인증 프로토콜들을 비교 분석하였다. 분석 결과에 따르면, 이 인증 프로토콜들은 NMA 기능을 제공하고 타원곡선 기반 전자서명을 사용한다는 공통점이 있는 반면에, SCA 기능 제공 여부, 인증서 사용 여부, TESLA 사용 여부 등에서 차이점을 보인다. 본 논문은 GNSS의 인증 프로토콜 공식 문서 또는 프로토콜을 제안한 논문을 참조하여 성능 분석을 진행하였는데, 비교 결과에 따르면, TBA 및 TTFAF가 가장 짧은 인증 프로토콜은 OSNMA인 반면에, 이들 두 성능 지표 시간이 가장 긴 프로토콜은 D1 기반 BeiDou-ECDSA이다. 또한, Chimera는 D1 기반 BeiDou-ECDSA의 TBA 및 TTFAF보다는 짧지만, 다른 인증 프로토콜들보다 NNA가 크기 때문에 BER의 증가에 따른 AER 및 $\overline{TBA}$, $\overline{TTFAF}$의 변화율이 큼을 확인하였다. 다만 BeiDou의 인증 프로토콜로 제안된 두 방법은 공인된 표준은 아니므로, 추후 BeiDou의 인증 프로토콜에 대한 공식 표준이 제정된다면 본 논문의 결과는 적절히 변경되어야 할 수 있다. 또한, 본 논문은 NMA에 대한 성능 비교만 진행하였으므로, 향후 연구로 SCA 및 NMA를 모두 포함하는 전체 인증 프로토콜에 대한 종합적인 성능 비교를 고려할 수 있다.

ACKNOWLEDGMENTS

This work was supported in part by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIT) (No. 2020R1A2C2013089) and in part by a grant from “Fundamental Research for Korea Satellite

Navigation System and Future Air Traffic Management" of the Korea Aerospace Research Institute funded by the Korea government (MSIT).

AUTHOR CONTRIBUTIONS

Conceptualization, D.Y.Jeon., T.Gaybullaev. and M.K.Lee.; methodology, D.Y.Jeon. and T.Gaybullaev.; validation, D.Y.Jeon., T.Gaybullaev. and M.K.Lee.; formal analysis, D.Y.Jeon. and T.Gaybullaev.; investigation, D.Y.Jeon. and T.Gaybullaev.; resources, J.H.Noh., J.M.Joo., S.J.Lee. and M.K.Lee; data curation, D.Y.Jeon. and T.Gaybullaev.; writing—original draft preparation, D.Y.Jeon.; writing—review and editing, J.H.Noh., J.M.Joo., S.J.Lee. and M.K.Lee; visualization, D.Y.Jeon.; supervision, M.K.Lee.

CONFLICTS OF INTEREST

The authors declare no conflict of interest.

REFERENCES

Air Force Research Laboratory Space Vehicles Directorate Advanced GPS Technology 2019, Interface Specification, Chips Message Robust Authentication (CHIMERA) Enhancement for the L1C Signal: Space Segment/User Segment Interface, IS-AGT-100. https://docs.google.com/viewer?a=v&pid=sites&srcid=Z3BzZXhwZXJ0Lm5ldHxsb2dhbi1zY290dC1jb25zdWx0aW5nfGd4OjEwOWY1NjgxNjI5ZDdhYmM

Caparra, G., Wullems, C., Ceccato, S., Sturaro, S., Laurenti, N., et al. 2016, Design Drivers and New Trends for Navigation Message Authentication Schemes for GNSS Systems, Inside GNSS. https://www.insidegnss.com/auto/sepoct16-WP.pdf

China Satellite Navigation Office 2019, BeiDou Navigation Satellite System Signal In Space Interface Control Document. http://en.beidou.gov.cn/SYSTEMS/ICD/201902/P020190227702348791891.pdf

China's State Cryptography Administration 2010, SM2 Elliptic Curve Public-Key Cryptography Algorithm, GM/T 0003-2012. https://www.chinesestandard.net/PDF.aspx/GMT0003.5-2012

ESA NAVIPEDIA – GPS Navigation Message, GPS CNAV-2 Navigation message [Internet], cited 2011, available from: https://gssc.esa.int/navipedia/index.php/GPS_Navigation_Message

ESA NAVIPEDIA – Galileo Navigation Message, Galileo INAV Navigation message structure [Internet], cited 2011, available from: https://gssc.esa.int/navipedia/index.php/Galileo_Navigation_Message

European Commission 2018, Galileo Navigation Message Authentication Specification for Signal-In-Space Testing-v1.1. http://www.kormanyablak.org/it_security/2021-07-04/GALILEO_OSNMA_TESLA.pdf

European Union Agency for the Space Programme 2021, OSNMA Typical Performance [PowerPoint slides], https://www.gsc-europa.eu/sites/default/files/sites/all/files/OSNMA_Typical_Performance.pdf

Fernández-Hernández, I., Rijmen, V., Rodriguez, I., Seco-Granados, G., Simón, J., et al. 2014, Design Drivers, Solutions and Robustness Assessment of Navigation Message Authentication for the Galileo Open Service, Proceedings of the 27th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2014), Sep 2014, Tampa, Florida, USA, pp.2810-2827. https://www.ion.org/publications/abstract.cfm?articleID=12532

Gamba, M. T., Nicola, M., & Motella, B. 2020, GPS Chimera: A Software Profiling Analysis, Proceedings of the 33rd International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2020), 21-25 September 2020, pp.3781-3793. https://doi.org/10.33012/2020.17717

Gaybullaev, T., Jeon, D.-Y., & Lee, M.-K. 2021, Poster: Performance comparison of GNSS navigation message authentication protocols, The 5th International Symposium on Mobile Internet Security (Mobisec 2021), 7-9 Oct 2021, Jeju, Korea

Jeon, D.-Y., Gaybullaev, T., & Lee, M.-K. 2021a, Performance Comparison of Authentication methods in GPS and Galileo, The Korea Computer Congress 2021, 23-25 Jun 2021, Jeju, Korea, pp.1208-1210. https://www.dbpia.co.kr/Journal/articleDetail?nodeId=NODE10583219

Jeon, D.-Y., Gaybullaev, T., & Lee, M.-K. 2021b, Comparative Analysis of Authentication Protocols of GPS, Galileo and BeiDou, 2021 IPNT Conference, 3-5 Nov 2021, St.John's Hotel, Gangneung, Korea, pp.119-122. http://ipnt.or.kr/2021proc/59

Margaria, D., Motella, B., Anghileri, M., Floch, J. -J, Fernández-Hernández, I., et al. 2017, Signal Structure-Based Authentication for Civil GNSSs: Recent Solutions and Perspectives, IEEE Signal Processing Magazine, 34, 27-37. https://doi.org/10.1109/MSP.2017.2715898

National Institute of Standards and Technology 2013, Digital

signature standard (DSS), Rep. FIPS PUB 186-4. http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf

Perrig, A., Canetti, R., Tygar, J. D., & Song, D. 2000, Efficient authentication and signing of multicast streams over lossy channels, IEEE Symposium on Security and Privacy, 14-17 May 2000, Berkeley, CA, USA, 56-73. https://doi.org/10.1109/SECPRI.2000.848446

Russian Space Systems OJSC 2016, GLONASS Interface Control Document, Navigational radio signal in bands L1, L2 (Edition 5.1). https://russianspacesystems.ru/wp-content/uploads/2016/08/ICD_GLONASS_eng_v5.1.pdf

Standardization Administration of the People's Republic of China 2016, Information security techniques – SM3 cryptographic hash algorithm. GB/T 32905-2016. https://www.chinesestandard.net/PDF.aspx/GBT32905-2016

Wu, Z., Liu, R., & Cao, H. 2019, ECDSA-Based Message Authentication Scheme for BeiDou-II Navigation Satellite System, IEEE Transactions on Aerospace and Electronic Systems, 55, 1666-1682. https://doi.org/10.1109/TAES.2018.2874151

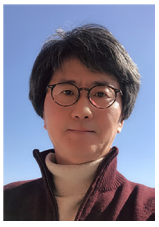
Wu, Z., Zhang, Y., Liu, L., & Yue, M. 2020, TESLA-based authentication for BeiDou civil navigation message, China Communications, 17, 194-218. https://doi.org/10.23919/JCC.2020.11.016

Da-Yeon Jeon is currently working toward the M.S. degree in Electrical and Computer Engineering at Inha University, Incheon, South Korea. She received the B.S. degree in Computer Engineering from the same university in 2021. Her research interests are information security and AI security.

Turabek Gaybullaev is currently working toward the M.S. degree in Electrical and Computer Engineering at Inha University, Incheon, South Korea. He received the B.S. degree in Information and Communication Engineering in 2019 from the Inha University in Tashkent (IUT), Uzbekistan. His research interests are cryptographic algorithms, information security, and blockchain.

Jae Hee Noh is a Ph.D candidate with the Department of Electronics Engineering at Chungnam National University in Korea. She received B.S and M.S degrees from Chungnam National University, Department of Electronic Engineering in 2017 and 2019, respectively. Her research interests include GNSS receiver, anti-spoofing techniques and message authentication.

Jung-Min Joo received his Ph.D. degree in Aerospace Engineering from Korea Advanced Institute of Science and Technology (KAIST) in 2015. He has been working at the Korea Aerospace Research Institute since 2004. His research interests include GNSS, SBAS, GBAS, and Ionosphere monitoring.



Sang Jeong Lee is a professor with the Department of Electronics Engineering, Chungnam National University, Korea. He received his B.S., M.S., and Ph.D. degrees from Seoul National University, Korea, in 1979, 1981, and 1987, respectively. His research interests include GNSS receiver design and robust control.

Mun-Kyu Lee received the B.S. and M.S. degrees in Computer Engineering from Seoul National University in 1996 and 1998, respectively, and the Ph.D. degree in Electrical Engineering and Computer Science from Seoul National University in 2003. From 2003 to 2005, he was a senior engineer at Electronics and Telecommunications Research Institute, Korea. He is currently a professor in the Department of Computer Engineering at Inha University, Korea. His research interests are in authentication, privacy-enhancing technology, applied cryptography, blockchain security, and AI security.