SBAS 信号認証機能の概要とプロトタイプの開発

航法システム領域　※坂井 丈泰，北村　光教，毛塚　敦

1　まえがき

GPS に代表される衛星航法システムは GNSS と総称され，従前より利用できる米国 GPS 及びロシアによる GLONASS のほか，最近では欧州の Galileo，中国の BeiDou，そして我が国による準天頂衛星システム（QZSS）を利用する環境が整ってきた。航空用途で GNSS を利用するには完全性（integrity：インテグリティ）を確保する機能の追加が必要とされ，これを行うのが補強システムである。ICAO（International Civil Aviation Organization：国際民間航空機関）は，人工衛星を経由して補強情報を伝送する SBAS（satellite-based augment- tation system）を規格化しており[1]，米国 WAAS，我が国の MSAS，欧州 EGNOS，そしてインドによる GAGAN がすでに稼働している。単一の GNSS 及び単一の周波数を補強対象とする現行の L1 SBAS に対して，複数の GNSS 及び周波数に対応した L5 SBAS の規格化が最近完了したところである。

一方，GNSS 信号についてはかねてより脆弱性が指摘されており[2]-[4]，近年は無線デバイス技術の進歩により「なりすまし」（spoofing）による攻撃が容易になっていることが問題視されている。この対策として GNSS 信号の認証機能を SBAS に追加する方式が議論されており，本発表ではこのための SBAS メッセージの検討状況を述べるとともに，L1 SBAS による実装のためのプロトタイプを開発したので報告する。

2　GNSS 信号の認証

GNSS 信号に対する攻撃のうち，偽信号によるなりすましはとりわけ問題視されている。原理的に攻撃対象が絞られはするが，攻撃者が意図する位置情報を攻撃対象の GNSS 受信機に出力させることができるのであるから，航空機の航法をはじめとする多くのアプリケーションにおいて利用者を混乱させ，損害を与えるか，さらには安全を脅かす懸念がある。

なりすましの対策の一つとしては，GNSS 信号の認証情報をユーザ受信機に提供する方式が考えられる[5]。ICAO においてもこうした認証機能を SBAS に付与する方式が議論されている[6]-[8]。SBAS では警報時間 TTA=6 秒とされていることから，平均認証間隔 MTBA=6 秒を満たすことが要件とされた。

2.1　基本的な仕組み

GNSS においてはユーザ受信機は GNSS 信号を受信するだけであるから，情報の流れは一方向であり，ユーザ受信機から GNSS 衛星に向けて信号を伝送することはない。このような場合に，ユーザ受信機が受信した GNSS 信号が正当なものであることを確認する仕組みとして，ディジタル署名技術を利用できる。

送信者に対応した公開鍵と秘密鍵の鍵ペアを用意しておき，通信内容のダイジェストに対して秘密鍵を適用した結果（これを認証符号 Message Authentication Code：MAC という）を署名情報として送信する。受信側では送信者の公開鍵でこれを復号し，受信した通信内容のダイジェストが一致すれば，送信者が正当であることを確認できる。これがディジタル署名方式の基本的な原理である。前提として，公開鍵から秘密鍵を推定することが実質的に（短時間では）不可能でなければならない。具体的なディジタル署名方式としては楕円曲線暗号による ECDSA（Elliptic Curve Digital Signature Algorithm）[9]を利用できる。

2.2　伝送方式

SBAS による認証機能の実現については，当初は L5 SBAS の Q-ch を使用する案が考えられたが，干渉による雑音の増加が懸念されたことから I-ch による実現性が検討された。ディジタル署名に用いる鍵は ECDSA 方式による一方，MAC の伝送にはハッシュ関数によるキーチェーンを用いる TESLA（Timed Efficient Stream Loss-Tolerant Authen-tication）[10]方式を採用する。これにより認証メッセージのサイズ

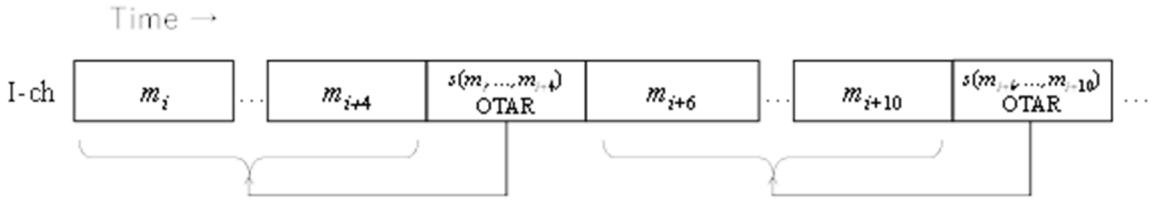

図 1　メッセージ送信順：TESLA 方式

を小さくでき，L5 I-ch により送信できる見込みが得られた。

さらに既存の L1 SBAS I-ch への適合性が検討され，一定の見込みがあることから，具体的なメッセージ構成が検討されている。SBAS のデータ速度は毎秒 250 ビットであり，メッセージ長 250 ビットのメッセージが毎秒 1 個ずつ送信される。各メッセージに格納できるデータサイズは 212 ビット（L1 SBAS）又は 216 ビット（L5 SBAS）である。

認証情報としては，SBAS メッセージに対する MAC のほか，MAC の検証に用いる公開鍵を送信する。後者は OTAR（Over-the-Air Rekeying）と呼ばれ，鍵ペアの安全性を確保するための措置である[7]。

2.3　TESLA 方式による認証情報

TESLA では，あるキーチェーンの i 番目の鍵を k_i としたとき，次の関係を満たすように所要数の鍵をあらかじめ生成し，生成順とは逆の順番で使用する。

$$h(k_i) \rightarrow k_{i-1}$$

$h(\cdot)$は一方向性ハッシュ関数である。受信側では，キーチェーンをたどっていくと必ずルートキーk_0 に到達する。このルートキーk_0 については公開鍵暗号により伝送する必要があり，これには ECDSA を使用する。所要の暗号強度を得るために，キーチェーンのハッシュ演算には 128 ビットのソルトを適用する。

TESLA では認証すべき情報及びキーチェーン中の鍵から MAC を生成し，鍵とともに送信する。受信側ではこの MAC の正当性を検証すればよく，MAC 生成鍵についてはハッシュ関数が，キーチェーンについては公開鍵暗号により送信されるルートキーが，それぞれ正当性を担保する。MAC を 16 ビット長として，5 メッセージ分の認証情報を 1 メッセージに収めて送信できるように認証メッセージが設計されており，これが直前に送信された 5 メッセージ（5 秒間）に対応する。TESLA 方式における認証情報と認証される SBAS メッセージの関係を図 1 に示す。

2.4　鍵の更新

信号認証に使用する鍵ペアが危殆化した場合，これを更新する必要がある。この更新を手動で行うことは現実的ではないことから，OTAR（On-the-Air Rekeying）と呼ばれる仕組みを実装することが考えられている[7]。

すなわち，認証用の鍵ペア（レベル 2）を更新する際には，公開鍵を ECDSA によるディジタル署名とともに送信する。この署名には，OTAR 用の鍵ペア（レベル 1）を用いる。レベル 1 の公開鍵については，あらかじめ受信機に内蔵させる。レベル 1 及びレベル 2 の鍵ペアに対して，TESLA のルートキーはレベル 3 の鍵情報として送信される。

3　MSAS への適用

前章に述べた信号認証方式を SBAS により実装する場合，認証メッセージの送信頻度に制約があることが問題になり得る。以前の検討[11]によりもっとも厳しいのは L1 SBAS の I-ch による場合であることがわかっており，現用の MSAS について実際の余裕帯域幅を求めるとともに，その拡大のための方策を検討した。

3.1　現状の空き伝送容量

現用 MSAS におけるメッセージの送信状況を調べるため，2022 年 8 月 7～13 日の 1 週間にわたり MSAS メッセージを受信し，メッセージタイプ（MT：Message Type）別に伝送帯域幅全体に対する占有率を求めた結果を表 2 に示す。

有意な情報を含まない MT63（ヌルメッセージ）は，全体の 17.18%を占めている。これを

表 2　伝送容量の占有率（現用 MSAS）

MT	送信回数	平均間隔 (s)	占有率 (%)
2～4	302,431	2.00	50.01
1, 7～28	198,460	3.05	32.81
63（空き）	103,909	5.82	17.18
合　　計			100

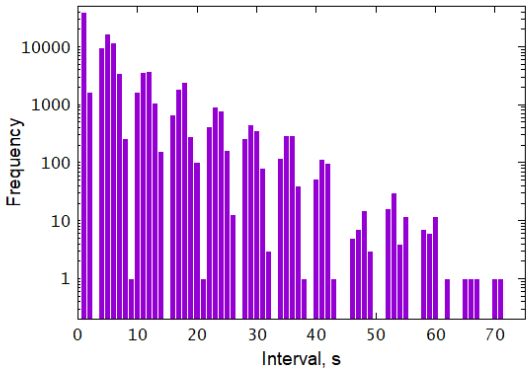

図 2　MT63 の送信間隔（現用 MSAS）

認証メッセージに置き換えれば 6 秒間に 1 メッセージ程度を送信できることになり，TESLA 方式では MTBA=6 秒をおおよそ満たせる見込みがあるものといえる。ただし，送信間隔の度数分布は図 2 の通りで，最大値は 71 秒であった。従って，単純に MT63 を認証メッセージに置き換えるだけでは，MTBA=6 秒を満たせない時間帯が存在する。また，6 秒毎に認証メッセージを送信することにすると，OTAR のための伝送容量は全体の 0.5%しか割り当てられず，毎時 18.5 メッセージ程度にしかならない。

3.2　必要な伝送容量

現在までに提案されている TESLA による認証方式[8]において，認証情報の送信に必要な伝送容量を検討した結果を表 3 に示す。MT20 は 6 秒毎に送信される認証メッセージ，MT21 はルートキー及び OTAR のための鍵情報を送信するメッセージとされている。

MSAS の例にならい，MT21 については最大送信間隔の半分の時間間隔で送信することにすると，認証情報の伝送には 28%程度の伝送容量が必要と見込まれる。現状の空き容量は表 2 の通り 17%余りであるから，何らかの方法により空き伝送容量を増やす必要がある。

表 3　認証メッセージの送信間隔

MT	鍵レベル	所要数	送信間隔 (s)	占有率 (%)
20	—	1	6	16.67
21	1	1	9	11.11
	2	7		
	3	4		
合　　計			3.60	27.78

表 4　空き伝送容量の検討（MT6 を使用）

MT	送信回数	平均間隔 (s)	占有率 (%)
2～4	60,487	10.00	10.00
6	100,811	6.00	16.67
1, 7～28	198,460	3.05	32.81
63（空き）	245,042	2.47	40.52
合　　計			100

3.3　空き伝送容量を確保する方策

SBAS のメッセージに含まれる情報のうちでもっとも高頻度に送信されるのは UDREI であり，MSAS の場合は MT2～4 で送信されている。MT2～4 は UDREI と高速補正情報を含んでいるが，一方で補強対象の全衛星の UDREI のみを送信する MT6 が用意されており，このメッセージを使用すれば MT2～4 の送信回数を減らせる可能性がある。

高速補正情報のタイムアウトは最大で 120 秒にでき，このとき他メッセージの例にならえば高速補正情報の送信間隔は 30 秒でよい。現状では MT2～4 を各 6 秒間隔で送信している（30 秒間で 15 回）が，これを 30 秒間で MT2～4 を各 1 回と MT6 を 5 回のあわせて 8 回にできる。

MT6 を使用する場合について空き伝送容量を検討すると，表 4 の通りとなる。高頻度に送信されている MT2～4 の伝送回数を減らすことで，大幅に空き伝送容量を増やせることが分かる。

4　プロトタイプの開発

現用 MSAS でも認証メッセージを送信できる見込みが得られたことを踏まえ，認証機能のプロトタイプを開発した。実装した認証メッセ

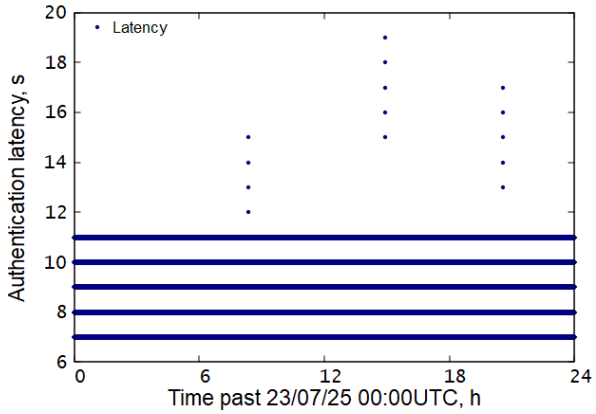

図 3　認証処理の遅れ時間

ージは現在までに提案されている TESLA 方式によるもので，MSAS が送信したメッセージのうち，MT2～4 の一部を MT6 に置き換えたうえで，MT20 を 6 秒毎に付加する。また，MT63 を MT21 に置き換え，これにより鍵情報を格納することとした。

ECDSA による鍵ペア（レベル 1 及びレベル 2）はあらかじめ生成して使用する。また，TESLA のキーチェーンは 1 週間を単位として設定した。開発に際しては暗号ライブラリ Libgcrypt を使用した。

MSAS が送信したメッセージに対して，プロトタイプを使用して実際に認証メッセージを生成し，認証遅れ時間（メッセージの受信後，認証されるまでの時間）を測定した結果を図 3 に示す。遅れ時間は設計通り 7～11 秒となるが，まれにアラートシーケンスの際には大きくなることが分かる。

5　むすび

SBAS による信号認証機能の実装について，ICAO における議論の状況を述べるとともに，L1 SBAS による実装の可能性を検討し，プロトタイプを開発した結果を報告した。現用 MSAS のメッセージ構成では伝送容量が不足するが，メッセージタイプ 6 を使用することで L1 SBAS でも認証機能を実現できる見込みである。引き続き，プロトタイプを使用して，雑音や攻撃に対する耐性を確認することとしたい。

参考文献

[1] Aeronautical Telecommunications, Annex 10 to the Convention on International Civil Aviation, International Standards and Recom-mended Practices, 7th Ed., ICAO, July 2018.

[2] John A. Volpe National Transportation Systems Center: Vulnerability Assessment of the Transportation Infrastructure Relying on the Global Positioning System, Aug. 2001.

[3] 水野勝成，“測位衛星への干渉・妨害，安全対策，” GPS/GNSS シンポジウム，pp. 248-251，東京，Oct. 2017.

[4] T.E. Humphreys, P.M. Kintner, Jr., M.L. Psiaki, B.M. Ledvina, and B.W. O'Hanlon (2009), “Assessing the spoofing threat,” GPS World, 20, 1, pp. 28-38.

[5] P. Enge and T. Walter, “Digital message authentication for SBAS (and APNT),” ION GNSS+ 2014, pp. 1328-1336, Tampa, FL, Sept. 2014.

[6] E. Chatre: SBAS authentication, ICAO NSP JWGs/2-WP/10, Montreal, June 2016.

[7] A. Neish, T. Walter, and J.D. Powell, “Design and analysis of a public key infrastructure for SBAS data authentication,” ION Pacific PNT, pp. 964-988, Waikiki, HI, April 2019.

[8] J. Dennis, T. Walter, J. Anderson, L. Cowles, I. Fernandez-Hernandez, and M. Mabilleau, “ Preliminary look as SBAS data authentica-tion requirements,” ICAO NSP JWGs/9-IP/20, Virtual, June 2022.

[9] NIST: FIPS PUB 186-4 Digital Signature Standard (DSS), July 2013.

[10] A. Perrig, R. Canetti, J. D. Tygar, and D. Song, “Efficient authentication and signing of multicast streams over lossy channels,” IEEE Computer Society Symposium on Research in Security and Privacy, pp.56-73, Berkeley, CA, May 2000.

[11] 坂井丈泰，北村光教，小田浩幸，“L5 SBAS による信号認証機能の基礎検討，” 第 65 回宇宙科学技術連合講演会，2G08，オンライン，2021 年 11 月.