

1 はじめに

衛星測位システム（GNSS：Global Navigation Satellite System）は、衛星が軌道情報や時刻情報を送信し、受信機が受信した信号から各衛星までの距離を計算することで、自身の位置情報だけでなく速度や時間を求めることができるシステムである。現在、米国が運用している GPS をはじめ、中国の BeiDou、ロシアの GLONASS といった様々な衛星が存在する。日本では GPS 互換の衛星である QZSS（Quasi-Zenith Satellite System）が運用されており、2025 年 3 月現在では 4 機の QZSS が順番に日本の天頂方向に位置するように配置されている。GNSS によって取得された位置情報や時刻情報は、自動車の自動運転技術やスマート農業の活用などの多分野で利用されており、国民の生活や社会インフラにも密接に関わっている[1]。一方、高高度を周回する衛星から送られてくる信号は非常に微弱であり、ジャミングやスプーフィングといった攻撃を受けやすい。特に衛星信号になりすました信号を送信するスプーフィングでは、受信機だけで検知することが難しい。衛星から送信される信号の仕様は公開されており、さらに USRP や HackRF といったソフトウェア無線機（SDR）の低コスト化が進んだことより、スプーフィングの危険性やその対策は喫緊の課題である[2]。

本研究は、ソフトウェア上で QZSS を含む GNSS 信号を生成するソフトウェアを作成し、無料公開することで、スプーフィング対策などの研究加速を図ることを目的としている。スプーフィング信号を実際に生成する方法として、GPS-SDR-SIM[3]とソフトウェア無線機を用いて疑似信号を生成する方法がある。しかし GPS-SDR-SIM は、GPS 信号生成のみを対象としているため QZSS には対応していない。さらに近年注目されている機械学習などのデータ駆動型手法を用いるためには、膨大なスプーフィングデータが必要になる。そこで本研究では、多くのソフトウェア無線機に対応している GPS-SDR-SIM を改良し、GPS と QZSS 信号が混在する環境を構築し、オープンソフトウェア化した。これにより、予算や機材が限られた研究機関が GNSS やスプーフィング対策の研究を行うことを容易にし、GNSS に関連する研究を加速させることが期待できる。

2 スプーフィング信号生成

2-1 スプーフィング信号生成システム全体像

スプーフィング信号生成システムの全体像を図 1 に示す。PC 上で仮想 GNSS（GPS と QZSS に対応した）ベースバンド信号を生成し、その信号をソフトウェア無線機である USRP で RF 信号に変換することで、スプーフィング信号を生成する。生成したスプーフィング信号を市販の GNSS 受信機（u-blox ZED-F9P）受信し、その結果を受信 PC 側に出力する。このことで、任意の場所、時間を指定した GNSS 信号（スプーフィング信号）を生成する。



図 1 USRP での信号実装概略図

2-2 スプーフィング信号生成（ソフトウェア）

（1）ベースバンド信号の生成

スプーフィング信号を生成するためには、実際の衛星信号になりすますため、GNSS の仕様を基に、各々の PRN で変調させた航法データを生成する必要がある。GPS-L1C/A におけるベースバンド信号は次式のように表すことができる。

$$S_{L1}(t) = \sqrt{2P_c} C(t - \tau) D(t - \tau) \exp(j2\pi f_t + \theta) \quad (1)$$

ここで、 P_c は C/A コードを搬送する信号の電力、関数 C は衛星の固有 PRN コード、関数 D は航法メッセージに対応する 2 値信号、 τ は衛星から受信機までの疑似距離に対応した時間遅延を表す。単位時間ごとに可視衛星の疑似距離を計算することによって、各衛星からの受信ベースバンド信号を生成できる。

(2) シミュレーション信号の生成

GPS のベースバンド信号をシミュレーションした信号を生成するウェアとして GPS-SDR-SIM がある。このソフトウェアは、NASA の公開アーカイブデータから取得したエフェメリスファイルとユーザの動きを定義したファイルから、GPSL1/CA のベースバンド信号ファイルを生成することができる。しかし GPS-SDR-SIM では、GPSL1/CA 信号のシミュレーション機能しか持たない。そこで、本研究では同じ帯域、変調方式を使用している QZSSL1/CA 信号も生成できるよう QZSS の仕様を基に、対応する PRN を拡張し、修正を加えた。GPS 及び QZSS のエフェメリスファイルは、図 2 に示す内閣府宇宙開発戦略推進事務局の公開アーカイブデータ[4]から取得することができる。また、NASA と内閣府宇宙開発戦略推進事務局が公開しているエフェメリスファイルにはフォーマットに差異が存在する。そこで、より実用的にスプーフィングを実装するため、単一のサイトから両方のエフェメリスファイルを取得できるよう修正を加えた。GNSS-SDR-SIM のオプションキーを図 2, 3 に示す。取得したエフェメリスファイルはそれぞれ、-e, -q キーで指定することができる。また、HackRF や bladeRF 等の SDR ではデフォルトのサンプルレートを 2.6 MHz で使用可能だが、NI-USRP ではサンプリングされたデータを取得できないため、-s キーで 2.5 MHz と設定した。2022 年 1 月 1 日、UTC 時刻で 12:00:00 に東経 134 度 06 分、北緯 34 度 29 分に位置する香川大学創造工学部の上空 1000 m であったかも受信したかのような状況でシミュレーションした出力結果を図 4 に示す。GPS と QZSS では QZSS 軌道条件、及びサービスエリア等の違いから格納される電離層情報に差異が存在する。本研究では、より実際の信号に近づけるため、GPS には GPS、QZSS には QZSS の電離層情報を格納している。図 4 上部の出力結果より、GPS 及び QZSS にはそれぞれ別の電離層情報が出力されていることが確認できる。また、図 4 下部の出力結果は、左から PRN、方位角、仰角、ユークリッド距離、伝搬遅延を表している。QZSS は PRN 番号から 192 を引き、頭に J を置いた値で出力している。J2 及び J3 衛星の仰角を見ると天頂方向に近い準天頂方向に位置していることが確認できる。また、仰角が低い衛星ほど、電離層遅延を受けやすく伝搬遅延が高いことが確認できる。

2-3 スプーフィング信号の RF 信号化

ソフトウェア無線機 USRP を動作させるソフトウェアとして、GNU Radio を使用した。GNU Radio は、米国の Eric Blossom が始めたオープンソースのソフトウェアツールキットである。GNU Radio で生成したベースバンド信号をスプーフィング信号として送信するブロックダイアグラムを図 5 に示す。スプーフィングを実行するプログラムは図 4 下部の三つのブロックから成る。「File source」では、GNSS-SDR-SIM で生成した GPS、及び QZSS のベースバンド信号を参照している。し

Data Select

Almanac
☐ QZSS+GPS Almanac ☐ QZSS Almanac ☐ GPS Almanac

Ephemeris(Rinex Extension version)
☒ QZSS Ephemeris ☒ GPS Ephemeris

Ephemeris
☐ QZSS Ephemeris ☐ GPS Ephemeris

Ultra Rapid Products
☐ QZU Orbit ☐ QZU ERP

Rapid Products
☐ QZR Orbit ☐ QZR Clock ☐ QZR ERP

Final Products
☐ QZF Orbit ☐ QZF Clock ☐ QZF ERP
☐ QZF Station Coordinate(in a day)
☐ QZF Station Coordinate(in a week)

Data Period

Start Epoch 2020 / 01 / 01

End Epoch 2024 / 01 / 01

Clear Search

図 2 エフェメリスデータ取得

```
C:\gnss>gnss-sdr-sim
Usage: gnss-sdr-sim [options]
Options:
-e <gps nav> RINEX navigation file for GPS ephemerides (required)
-q <qzss nav> RINEX navigation file for QZSS ephemerides (required)
-u <user motion> User motion file (dynamic mode)
-g <nmea_gga> NMEA GGA stream (dynamic mode)
-c <location> ECEF X,Y,Z in meters (static mode)
e.g. 3967283.154,1022538.181,4872414.484
-l <location> Lat,Lon,Hgt (static mode) e.g. 35.681298,139.766247,10.0
-t <date,time> Scenario start time YYYY/MM/DD,hh:mm:ss
-T <date,time> Overwrite TOC and TOE to scenario start time
-d <duration> Duration [sec] (dynamic mode max: 300, static mode max: 86400)
-o <output> I/Q sampling data file (default: gsssim.bin)
-s <frequency> Sampling frequency [Hz] (default: 2600000)
-b <iq_bits> I/Q data format [1/8/16] (default: 16)
-i Disable ionospheric delay for spacecraft scenario
-v Show details about simulated channels
```

図 3 オプションスクリーン

```
C:\gnss>gnss-sdr-sim -e brdc0010.22h -q brdc0010.22q -t 2022/01/01,12:00:00
-l 34.29288,134.06399,1000 -s 2500000
Using static location mode.
xyz = -3669148.8, 3791032.6, 3573897.0
lh = 34.292880, 134.063990, 1000.0
-----GPS Ionospheric Data-----
1.118e-08 -7.451e-08 -5.960e-08 1.192e-07 ION ALPHA
1.167e+05 -2.294e+05 -1.311e+05 1.049e+06 ION BETA
-9.31322574620e-10 -1.77635683900e-15 233472 2191 DELTA-UTC
18 LEAP SECONDS
-----QZSS Ionospheric Data-----
1.118e-08 -5.215e-08 -2.980e-07 0.000e+00 ION ALPHA
1.024e+05 -3.277e+04 -1.376e+05 -6.226e+06 ION BETA
1.86264514920e-09 0.00000000000e+00 180224 2191 DELTA-UTC
18 LEAP SECONDS
-----
Start time = 2022/01/01,12:00:00 (2190:561600)
Duration = 300.0 [sec]
01 208.3 58.8 20651079.9 1.7
03 172.1 5.0 25238184.2 5.0
07 256.1 46.0 21481995.9 2.0
08 38.5 53.4 21203298.7 1.8
10 47.4 11.9 24691217.0 3.9
16 120.5 19.9 23969517.8 3.3
17 265.3 3.4 25431936.7 5.9
21 80.5 85.5 20337794.4 1.5
22 155.4 22.6 23275602.2 3.1
27 64.0 26.0 23166571.0 2.9
30 292.3 34.6 22383545.4 2.4
J2 156.3 73.5 37523092.0 1.5
J3 222.0 88.7 38343928.1 1.5
J7 192.3 49.4 37113152.4 1.9
Time into run = 300.0
Done!
Process time = 247.3 [sec]
```

図 4 出力結果

かし、生成したベースバンド信号はバイナリファイルのint型であるため、そのままでは複素型のRF信号として送信することができない。そのため、「IChar To Complex」でcomplex型に型変換をする。その後、「UHD:USRP Sink」で変換したベースバンド信号をアップコンバートし、スプーフィング信号として送信する。ここで、信号送信時の中心周波数、及び送信時ゲインは図5上部のvariableブロックを参照している。なお、図5上部のOptionsはGNU Radioのオプション設定を示しているが、今回はデフォルト設定を使用した。また、今回の実験に使用した機器の構成は図1と同じである。生成された信号を評価するためには実空間中を伝搬する真のGNSS信号を排除する必要がある。そこで今回の実験では同軸ケーブルによって接続可能なGNSSモジュールであるu-blox社製のZED-F9Pを用いる。また信号解析ソフトは高性能GNSS評価・グラフィック表示可能なu-center2を使用する。

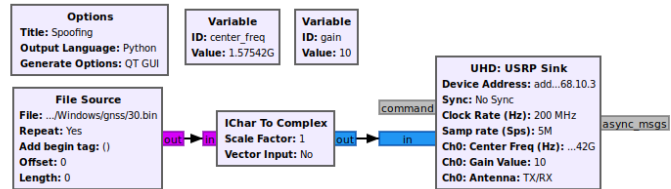


図 5 スプーフィング信号生成ブロック

3 スプーフィング信号生成結果と評価

受信機が十分に安定して信号を捕捉し、測位した3分後の出力結果を図6から8に示す。図6に示すマップ画面では位置情報を香川大学創造工学部と出力していることが確認できる。図6は受信機の緯度、経度、高度、速度、及びUTC時刻を表している。緯度、経度を確認すると、指定した北緯34度29分、東経134度06分、また、UTC時刻では指定した12:00:00から3分後の結果が出力されている。しかし、高度は40m程ずれていることが確認できる。この理由は、u-center2側では海拔高度として高度を出力しているのに対し、シミュレーション信号では生成時に楕円体高からの高度を入力していることに大きく起因する。そこで、以下にジオイド高を考慮した誤差について考察する。国土地理院の測量計算サイトによると、香川大学創造工学

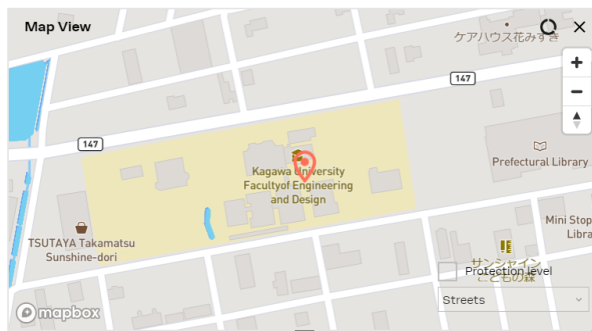


図 6 マップデータ

Data View
Fix mode
3D-fix
TTFF
Longitude
134.0639965°
Latitude
34.2928885°
Altitude
962.400 m
Velocity
1.063 m/s
UTC time
12:03:00
3D acc. (0-50)
2D acc. (0-50)
PDOP (0-10)
1.910
HDOP (0-10)
1.180
Used in navigation
8/8
Not used in navigation
-/8
Not tracked
-/8

図 7 位置情報

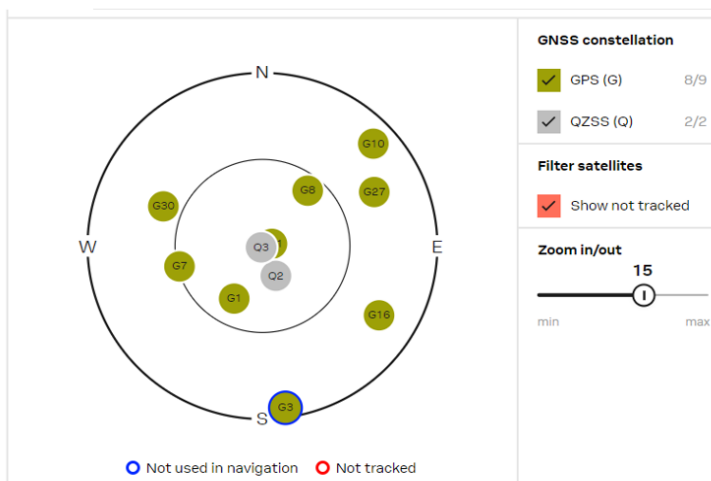


図 8 受信衛星配置

部周辺のジオイド高は36mであるため、それを考慮すると

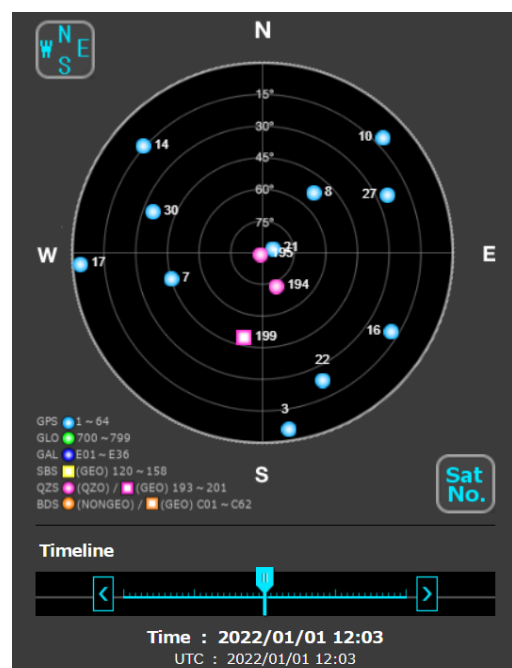


図 9 内閣府提供の衛星配置

誤差は4m程度(40-36)となる。さらにGNSSでは一般に水平方向(緯度, 経度)より垂直方向(高度)の方が, 測位精度が悪いことが知られている。これは, 受信信号強度の強い衛星, つまり電離層の影響が小さい仰角の高い衛星を利用するため, 結果として測位点と衛星の配置関係が偏るためである。また, 速度に関しては位置情報を推定していく段階で算出した結果と考えられる。図8は受信機が出力した衛星配置, 図9は内閣府が提供しているGNSSVIEWアプリを使用して, 位置, 時刻を合わせた衛星配置である。図9のQZSS番号はPRNを表しているため, 192を引いた値が左部の衛星番号となる。両者を比較すると, シミュレーションで生成したGNSS信号の受信結果は, 仰角の低い衛星について捕捉できていない点を確認できる。これは受信機が信号強度の高い信号を基に位置座標を測位するため, 電離層遅延を受けやすい低仰角の衛星の信号を捕捉しなかったと考えられる。ただし, 仰角の低い衛星信号は一般に位置推定に使用しないため, 作成したGPS及びQZSSスプーフィング信号作成は成功していると判断できる。

4 おわりに

本研究では, スプーフィング対策の研究活性化を目的に汎用 SDR 機で生成可能な GNSS 信号生成プログラムを作成し, 公開した[5, 6]。特に QZSS に対応した無料ソフトウェアとして公開しており[6], USRP のような SDR 機を持つ研究機関では, git-hub からダウンロードしてコンパイルするだけで, 生成可能である。本研究では, 生成したスプーフィング信号に対するデータ駆動型検出方法の構築を目指していたが, 成果を期間中にまとめることができなかったため, 今後の研究課題としたい。また, スプーフィング対策として, 2024 年 4 月から信号認証サービス[7]が開始されたため, それを含めたセキュリティに関する研究への発展も検討したい。

【参考文献】

[1] Y. Tsunoda and T. Okubo, “Research of the importance of GPS timing affecting critical infrastructure,” IPSJ SIG Technical Report, Vol. 2019-CSEC-84, No. 1, pp. 1-8 (2019)

[2] M. Lianxiao, Y. Lin, Y. Wu, and Z. Long, “A Survey of GNSS Spoofing and Anti-Spoofing Technology,” Remote Sensing, Vol. 14, No. 19 (2022)

[3] Takuji Ebinuma, GPS-SDR-SIM git-hub, <https://github.com/osqzss/gps-sdr-sim>

[4] 内閣府宇宙開発戦略推進事務局, “パフォーマンススタダード PS-QZSS)) ,” <https://qzss.go.jp/en/technical/download/pdf/ps-is-qzss/ps-qzss-003.pdf?t=1676424083242>

[5] 河崎, 石井, “汎用 SDR 機を用いた GPS 及び QZSS スプーフィング信号生成,” 電気学会 C, 144 巻, 8 号, pp. 793-798, 電気学会, 2024

[6] GitHub: “gnss-sdr-sim”, <https://github.com/Yuta811x/gnss-sdr-sim> (2022)

[7] 信号認証サービス, https://qzss.go.jp/overview/services/sv14_sas.html

〈発 表 資 料〉

題 名	掲載誌・学会名等	発表年月
汎用 SDR 機を用いた GPS 及び QZSS スプーフィング信号生成	電気学会論文誌 C, 144 巻, 8 号, 電気学会	2024 年 8 月
GNSS のミーコニングの実装評価	電気・電子・情報関係学会四国支部連合大会	2024 年 9 月
GNSS 受信機による CLAS と RTK 測位の精度比較	電気・電子・情報関係学会四国支部連合大会	2024 年 9 月