SpaceOps-2025, ID # 1 (104)

The protection function of GNSS assistance in the ground-to-Space

Jamel Metmati[a]

[a] *Cyber Science Institut, ISAE-SUP AERO, France*, *Djamel.METMATI@ext.isae-supaero.fr*

Abstract

The GNSS assistance depends on the constellation and the availability of stations on the ground to catch the signal from the horizon and to cover an area. One of the functions is to delivered the time for a network. The sources of time is the element for the telemetry tasks and some administration functions for the facilities on the ground, to maintain the coherence of the system, to ensure the sustainability of the satellites themselves. The protection function of GNSS assistance means to consider the connectivity of Space segment for the networks for a specific needs linked with the GNSS assistance. The satellites use an internal clock with a GNSS references and the lost of these parameters produce the operational effects for their management and the slot availabilities for the use of their sensors by the stakeholders. This parameter gives the workflow metrics for the cycle of data processing in a network on terms on seconds, milliseconds, nanoseconds. And as the computation is limited in Space by the power available, the data transmission requires the protection of the buffer parameters to secure the bit management for the satellites and its dependancy on the ground.

Keywords: computation, synchronization, constellation

Acronyms/Abbreviations : GNSS, PTP, GPS, RINEX

1. Introduction

The case of Space segment is a point for it considers the protection of the times function in the GNSS assistance to manage the data from Space to the network on the ground. An operational service which uses the GNSS assistance for its function. It considers the protection of the assistance itself mainly the time function and this function for a operational service expected on the ground. The use case choosen considers an exchange of data using GNSS function with the need of synchronisation to make the communication for Space surveillance and tracking an object in Space. This case shall be considered by the connection to the Internet to be able to send the data to another sites. The Internet network uses the connection on the ground and by Space directly because of the advantage to get the communication in the isolated sites.

2. Material and methods

The methodology is to consider the definition of the GNSS assistance for the ground, mainly, for the support of networks. The configuration parameters is to notice the NTP, SNTP, PTP, IRIG service in the network management to ensure the work of system. It concerns the DCF77 and the IEEE 802.1AS. The constraint to send data to the ground with the fragmentation technique due to the memory capacity of the embebbed system produce the re-computation to provide times. The signal itself is not fragmented. The point is the concern of the time server. The signal contains a modulation and a code (BPSK or other) with the several type of data including ephemeride, almanach, pseudorange. This last parameter computes the distance between the timer server and the satellite.
The rest of the data concerns the position of satellites, time precision, and general information about the GNSS constellation. The time server uses these datas to synchronize its internal clock by nanosecondes. The buffer can happen even if the signal is received continuously in order to maintain the signal on real time. The function of this buffer provides the check processing for the integrity of data, the synchronization with the internal clock and the corrections. It considers this step as protection function of GNSS assistance for the critical point is reached if the signal is spoofed or degraded due the position of the satellites. The buffer acts as the assistance to correct the anomalies providing the re-synchronization between the ground-to-Space. The algorithm of synchronization

considers the PTP or NTP protocols depending on the network. The protection function of GNSS assistance by the buffer in the time server should be completed by the integrity of its works to ensure that the algorithm of synchronization works without the wrong input of re-computation in case of spoofing and degradation of the signals.

3. Theory and calculation

3.1 GNSS Frame structure

The purpose is to provide an achitecture and the network configuration ground-to-Space to intent the design of the protection function. The requirements should taken account the ECSS data format, the processor configuration, the mechanisms of the exchange between the network equipments and the framework of NIS regulations [1]. Other supports can be used depending on the need to protection for the operational service. The scenario considers a data exchange of 1Mbits from an optic telescope using the GPS assistance function to coordinate several telescope for observation and the capacity to forward data to the endpoints as the data centers and the web users.
The calculation integrates the MTU of the date frame including the GNSS assistance to compute the function and the synchronisation of the network on the ground segment.
The scenario considers the frame of 1200 octects (figure 1) which includes the data from times server and its re-computation to the Internet to send data to a remote site. To test the frame, the Scapy tool would be used to build the packet and to test it in a simulated system model to check the protection function of the GNSS sequences. The strategy to define the function is linked with the authentication, the certificates, the configuration of the times server and the integrity control of the signal from the GNSS constellation. For the ground-to-Space uses in order to relieve the data processing, the protection function includes the parameters of the position, the length and the description of the frame without consideration of the operational services which integrate the functionalities of authentication. The function is marked by in the times server itself able to consider the multi-system signal architecture to ensure the quality of the observation (figure 2).

Position	Length (octets)	Description
0-1	2	Type of Frame
2-5	4	Length of Frame
6-9	4	Sequence Number
10-11	2	Error Code
12-69	58	GNSS data
70-109	40	Times Server parameters
110-1195	1086	User data
1196-1199	4	Checksum

Figure 1 : Frame structure example

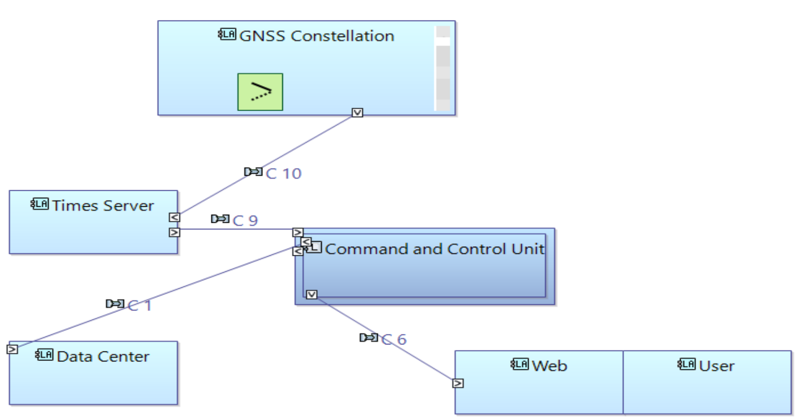

Figure 2 : Model GNSS Assistance

The GNSS constellation considers the Galileo, EGNOS, Beidou, Glonass satellites. The GPS scenario is included in the time server equipment with NTPSec software. The Data Center represents the datas collected from the telescope which requires the times to manage and spread them through the networks via the Internet or user using the network as a support to professional purpose. The time server gets the GNSS information via the RINEX files which contain information about the observations of pseudorandom, carrier phase, Doppler and navigation signal.

They are also used for post-processing of GNSS data, correcting errors and improving the accuracy of computed positions. RINEX [2] files can be used to analyze and correct positioning and navigation data. They can also be used to check the accuracy of GNSS receiver clocks and time servers. Then, RINEX files play a crucial role in the collection, exchange and processing of GNSS data, while time servers use this data to ensure accurate and reliable time synchronization. RINEX (Receiver Independent Exchange Format) files are protected in several ways to ensure the integrity and security of the GNSS data they contain:

- The integrity check can include checksums (checksums) to verify data integrity. This allows to detect any alteration or corruption of files during their transfer or storage.
- The encryption can be encrypted to protect sensitive data from unauthorized access. Encryption ensures that only authorized persons can read and use the data contained in the files.
- The authentication can be digitally signed to ensure their authenticity. The digital signature is used to verify that files come from a reliable source and have not been modified.
- The access control: RINEX file management systems can implement access controls to restrict access to files only to authorized users. This includes the use of passwords, digital certificates and other authentication mechanisms.
- The backup and redundancy : RINEX files can be backed up regularly and stored in redundant locations to avoid data loss in the event of hardware failure or disaster.

The scenario to consider the GNSS protection function means to take care about the RINEX (Receiver Independent Exchange Format). As the RINEX files are text files that contain GNSS observation data, the transmission over a network with an MTU (Maximum Transmission Unit) of 1200 bytes will fragment into multiple frames to fit the maximum frame size. The RINEX files are divided into segments of 1200 bytes or less. Each segment is encapsulated in a network frame with the appropriate headers for the communication protocol used. If the RINEX file is larger than the MTU, it will be split into multiple frames. Upon receipt, frames are reassembled to reconstruct the original RINEX file. The communication protocol used ensures that frames are received in the correct order and without data loss.

In the scenario tested, the fragmentation of RINEX file into 1200-byte frames following the sequence as Frame 1 = 1200, Frame 2=1200, Frame N < 1200. The frame over the network after the data received could contain the RINEX in the payload. The frame structure considers the header parameters with source address (6 octets) and destination source (6 octets), the type (2 octets), the header of the frame considering the IPVv4 contains the other parameters.

Version : 1 octect
Type of service : 1 octect
Identification : 2 octects
Flags and offset : 2 octects
TTL : 1 octect
Protocol : 1 octect
Checksum : 2 octects
Source Adress : 4 octects
Destination Adress : 4 octects
UDP header : 8 octects (source port : 2 octects, Destination source : 2 octects, Length: 2 octects, Checksum: 2 octects)
Rinex data : 1200 octects

Figure 3 : Frame Example with RINEX data

The data of the GNSS receiver shall be combined with the RINEX data from the observation. The use case of the observation is the Apophis Asteroid data. As described on the figure, the RINEX format for one GPS constellation can provide the XYZ position [3].

```
OBSERVATION DATA    M (MIXED)         RINEX VERSION / TYPE
TEQC  2010Mar01  NASA-GSFC         20100301 000128 UTC PGM / RUN BY / DATE
MARKER NAME     APOPHIS_OBS
ARMM 9026       STATION ID
4189237.2210  1108364.2190  4784324.1900              APPROX POSITION XYZ
2025    03    02    18    00    00.0000000    GPS        TIME OF FIRST OBS
XXX  XX   XX   XX  XX  XX.000000    XXX        OTHER OBSERVATION
                                        END OF HEADER
  02  25  03  02  18  00  00.0000000  0  0  0  0  0  0  0  0  0  0  0  0  0  0
  02  25  03  02  18  00  30.0000000  0  0  0  0  0  0  0  0  0  0  0  0  0  0
  02  25  03  02  18  01  00.0000000  0  0  0  0  0  0  0  0  0  0  0  0  0  0
```

Figure 4 : APOPHIS GPS RINEX

In the context of multi-system GNSS, it considers the RINEX files including the other constellation like Galileo, Glonass, Beidu.

```
3.04          OBSERVATION DATA    M (MIXED)          RINEX VERSION / TYPE
TEQC  2025Mar05  My Observatory       20250305 120000 UTC PGM / RUN BY / DATE
MARKER NAME      APOPHIS_OBS
MARKER NUMBER   00123
OBSERVER / AGENCY    J.DOE      / My Observatory Team
REC # / TYPE / VERS  12345XYZ  GNSS Receiver Model       3.04
ANT # / TYPE         67890ABC  GNSS Antenna Model
APPROX POSITION XYZ  1234567.89  987654.32  4567891.78
ANTENNA: DELTA H/E/N 1.2340    0.5678    -0.8912
TIME OF FIRST OBS     2025    03    05    12    00    00.0000000 GPS
SYS / # / OBS TYPES  G 16 C1C L1C D1C S1C C2W L2W D2W S2W
                     R  8 C1C L1C D1C S1C
                     E 12 C1X L1X D1X S1X C5X L5X D5X S5X
END OF HEADER
> 2025 03 05 12 00 00.0000000  0 G12 G15 G18 G21 R05 R10 E07 E12
G12  23456789.123  12345678.123  12345.123  45.123
G15  22334455.678  11223344.567  67890.567  50.567
R05  34567890.456  23456789.456  78901.456  65.456
E07  33445566.789  22334455.789  12300.789  70.789
> 2025 03 05 12 00 30.0000000  0 G12 G15 G18 G21 R05 R10 E07 E12
G12  23456789.223  12345678.223  12345.223  45.223
G15  22334455.778  11223344.667  67890.667  50.667
R05  34567890.556  23456789.556  78901.556  65.556
E07  33445566.889  22334455.889  12300.889  70.889
```

Figure 5 : APOPHIS GNSS RINEX

3.2 GNSS Buffer frame

In this file, each satellite G12, G15, R05, E07 include the pseudorange, the carrier phase, the Doppler and the signal/noise ratio values. These values used by the potential buffer of the times server introduce its management in the algorithm of synchronization after a loss or a degradation of the signal. In this use case mentioned, the

observation data considers the C = pseudorange, L = phase de porteuse, D = Doppler, S = signal-to-noise ratio for each satellite of GNSS constellation : G for GPS, R for GLONASS, et E for Galileo.
This file contains information on the observation of the asteroid Apophis, including the approximate position of the telescope, date and time of observation, and GNSS observation data. The receiver gets the multi-system signal from the satellites and the buffer of time server takes account of the constellation to re-compute the signal.
The integrity of the synchronization needs the markers to ensure the sequence is preserved. It exists from the internal clock of the times server and the buffer of times when the signal doesn't work. The derives noticed are mitigated thanks these parameters but the quality of the buffer of times is critical for the computation of the synchronization above all with multi-frequency available on the receiver with several GNSS constellation. The varieties of filter of Kalman, H-infinity or Monte-Carlo methods ensure the process of prediction to re-compute the signal. The buffer of times is usually stored in RAM, flash memory and can be managed through the external module.
The optimized buffer of times consists to get AI engine to be able to maintain the data or not depending on the availability of the GNSS signal.
This provide the predictivity close to the status signal avoiding the re-computation with the values of the derives too high. To do that from the PTP version, the methods uses the header of the buffer of times including three parameters : "ptpVersion", "sequenceId", "TimeStampQualityIndicator" "good" for Signal correct from source recovery. Then, it adds the control bits to garantue the integrity of the header. The value of the header is evaluated between 10 and 14 octects.
The AI engine controls from external module compute the sequence of the start and the end of the header including the time of data storage in the memory depending on a signal incoming or not. The advantage is double for the signal itself and the alignement with the OT and IT network on the infrastructure using the timer server and its potential buffer. The agent is configured to be re-code with new parameters depending on the other equipments applied.
The methods linked with redundancy of the system, the anti-jamming, the filters applied for the receivers, the cryptology are already included in the protection function. The point is the way to consider the function in the context of multi-system to get the guarantee to maintain the protection of the data encapsuled in the signal received on the infrastructure. As the function of the telescope is to collect images from Space to detect an asteroid, the quality of the GNSS protection function would be a factor to locate and the provide high precision for the detection. The collect is viewed through the tools like AstroPlanner and Maxim DL to manage the observations.

4. Results and Discussion

The way to consider the protection function is the times computation and the position of the observers (telescopes, satellites). More the times can be computed with the assets from the ground and in Space, more is possible to consider the precision of an effect. In the use case of protection of the function for the asteroid, it means without the protection, the trajectory is no more accurate to be taken account with precision in the IT and OT networks. Considering the data-center available to store the data, the times must be used in these networks.
The point is to note that the time marks the management of the network on the ground. The protection function shall be kept in the network through the protocol PTP or NTP played by the network equipments to maintain the coherence of times. As these equipments are connected with the times server, the need of synchronisation is constant. The protection function is also linked with the capacity to retain the synchronisation in the work flow of data. It depends on the time of transit for the data and the features of the correction (immediate, jump, drift). The transit considers the packets management of the network configuration : hops, banwidth, congestion, fragmentation with the MTU value. The techniques to preserve the statement to mitigate considers the techniques following via the building agent [4]:

- the configuration of the switchs and the routers to ensure the data from timer server with the parameter of synchronisation with the lower congestion level (sub-network) via the routing segment [5]
- the geographic position of the time server with the other equipments to maintain the requirements of the data quality for the transmission of synchronised GNSS datas
- the choice to data transmission protocol in which UDP increases the speed and TCP the reliability
- the buffer storage stored in the multiple location in the main time server with the copies of the buffer working with an synchronisation algorithm to ensure the integrity of the re-start the signal if the main buffer is lost after the loss or the degradation of GNSS signal.

6. Conclusions

The protection function of GNSS assistance is the capacity to manage the time server and the buffer integrity to ensure the continously of the signal for the applications on the ground. The multi-system supporting by the receivers from the GNSS constellation requires more attention about the sequence of synchronization and the need to alert the drifts more precisely via the agent building to monitor them computable on Space HPC infrastructure.

References

Reference to a regulation publication:
[1] DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)

Reference to a journal publication :
[2] C. Noll, Y. Bock, H. Habrich and A. Moore, "Development of data infrastructure to support scientific analysis for the International GNSS Service", Journal of Geodesy, Feb 2009, pages 309-325, DOI 10.1007/s00190-008-0245-6.

Reference to a website:
[3] https://gitlab.com/sgl-ut/GPSTk/-/blob/main/data/rinheaddiff/RINEX3_OBS_1.txt?ref_type=heads
[4] https://github.com/CSI-Space/Asteroid

Reference to a book:
[5] "Industrial Communication Technology Handbook", 2nd Edition, CRC Press, Richard Zurawski", December, 2017.