Distributed and layered approach for GNSS signal monitoring and threats detections

Marc POLLINA
M3 Systems, 26 Rue du Soleil Levant 31410 Lavernose (F) , +33 5 62 23 10 80
pollina@m3systems.eu
Olivier DESENFANS
M3 Systems, 1,3 Chemin du Stocquoy, 1300 Wavre (B), +32477382497
desenfans@m3systems.eu -

Abstract:

Keywords: GNSS vulnerabilities & threats, autonomous applications, integrity, GNSS receiver KPI's

The radio-navigation signals generated by the various GNSS satellite constellations (GPS, GALILEO, GLONASS, BEIDOU,..) are becoming essential for most of our daily activities. In the future this will even increase since it is expected that GNSS role will be essential in the transport domain for the development of autonomous systems.
Although modern GNSS satellite system provide high level of performances with respect to signal in space and correction of atmospheric propagations there are local vulnerabilities namely (jamming, multi-path, spoofing) that may degrade the performances or even cause the unavailability of GNSS positioning.
Consequently it is essential to address the possible solutions that may be used to better manage these threats. The issue of GNSS vulnerability has become a hot topic since few years, in particular with jamming cases reported in airport areas or spoofing of large vessels.

In this paper we propose to address threats detection and mitigation on GNSS by addressing this issue at system level when defining the application architecture. Our proposed approach is to increase the signal monitoring capabilities by using the distributed nature of the GNSS applications (mobiles, local control station, regional/global infrastructure) but also by getting observable at different levels of the GNSS signal processing chain (RF front end, Baseband, PVT). It is expected that with the increased capabilities of software radio technology and increased real time data link capabilities such as 5G it will be possible to develop applications that are using this approach to become more resilient to GNSS threats.

We will first address two GNSS applications that illustrate typical cases of “critical applications” , in other words those application that require an high level of confidence in GNSS positioning (integrity). First application, “E-trackair” is deployed at Toulouse and Bordeaux airports and is dedicated to the geolocation of airports vehicle. The main scope of the application being to avoid “runways incursions” that are a major risk to the aircraft. The second application is a long range drone application that has been demonstrated in the frame of a GSA project called “SKYOPENER”. In this case the objective is to perform inspection of large infrastructures such as electrical lines or railways requiring safe navigation over distances greater than 200 km. In these two cases we will show how to use the mobiles capabilities coupled with ground stations at local and global level to monitor the GNSS signal quality. This is a key to better characterize the operational environment and to derive the impact on the quality of service seen by the users.

Secondly we will propose a layered architecture of GNSS applications that enables the proper observability of the signal characteristics and the elaboration of relevant KPI's. The proposed breakdown is organized in 4 layers : PVT, raw data, post-correlation, I/Q samples.

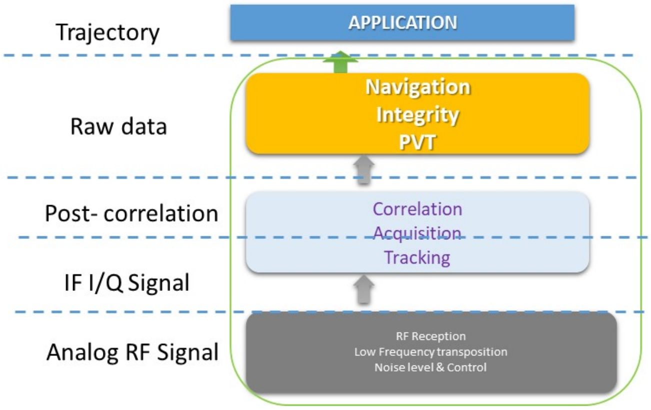

Fig 1 : GNSS receiver layered breakdown

At each we will illustrate the effect of different types of vulnerabilities and we will propose possible ways of detecting and mitigation them.

Finally we will illustrate few technical achievements based on the use of National Instrument software radio solutions (PXie platforms) that demonstrate the technical feasibility of our proposed concepts.

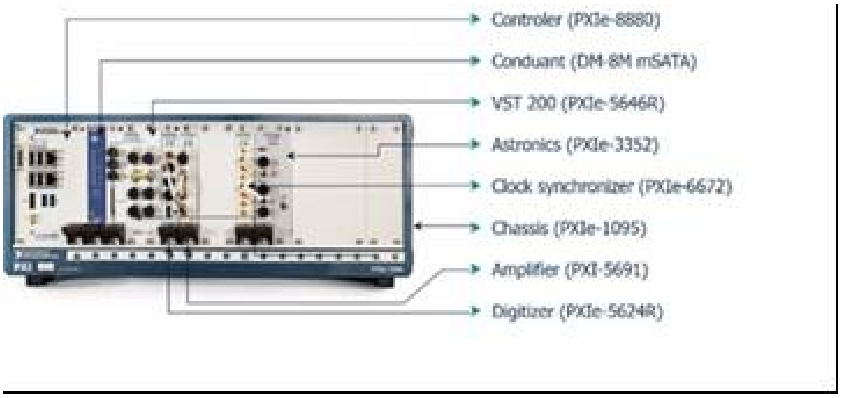

Fig 2 : Software radio-platform for GNSS signal monitoring

We will highlight two cases:

- Test bench for evaluation of GNSS authentication algorithms : the test-bench integrates a source of authenticated GNSS signals, a spoofing device, a RF front end, GNSS receivers and a platform used to test authentication software.
- EGNOS V3 signal monitoring : the equipment checks the compliance of the RF signal-in-space quality metrics in real-time with respect to predefined thresholds by means of KPIs