White paper

Sources of RF Interference and how to diagnose and mitigate?

Abstract

Centimetre-level RTK or PPP positioning requires high quality GNSS measurements. By virtue of their low power however, GNSS signals are prone to interference with the first symptom often being a loss of RTK or PPP position output. In the case of marine applications, disruptions caused by loss of precise positioning, as well as being costly, can also have dangerous consequences. This paper discusses various sources of interference and details the approach of Septentrio to both diagnosing and mitigating the effects of GNSS interference.

Introduction

GNSS signals are transmitted with a power equivalent to that of a standard light bulb. Unlike the light from a bulb however, GNSS signals are expected to travel more than 20,000 km and still arrive fit for high-precision position calculations. In most cases, the satellite signals arrive relatively unscathed albeit with very low power. With GNSS signals barely distinguishable from the thermal noise, as Figure 1 shows, it is relatively easy for them to be disrupted by a nearby interferer transmitting at the milliwatt level.

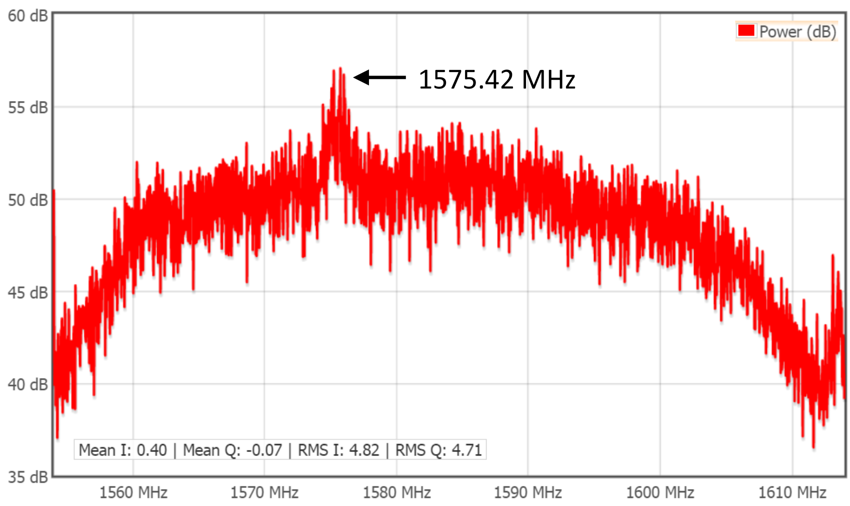

Figure 1: spectrum plot of the L1 band without interference with the GPS L1C/A central frequency indicated

The most precise cm-level positioning modes, RTK and PPP, use not only the code information modulated onto GNSS signals but also the phase of the signal itself. In the presence of interference, phase-based positioning modes are the first to suffer as these require the highest quality measurements.

Maritime applications are increasingly employing high-precision GNSS positioning and for these users, any downtime in RTK or PPP availability can have expensive repercussions: a large dredging operation loses tens of thousands of euros for every hour it lies idle.

Sources of interference

The ramifications of interference are never pleasant and for marine operations they can be particularly serious. Large marine vessels lack the manoeuvrability of those on land and, coupled with the inherent danger of an offshore environment, the stakes are far greater.

Marine operations are subject to many sources of potential interference: malfunctioning radio transmitters, amateur radio transmissions, military navigation aids and even intentional jamming. The intermittent nature of most jamming events makes them difficult to detect and even more difficult to diagnose. The following section details several cases of interference encountered in the field.

Radio amateurs

On a construction site in Ostend harbour in Belgium, shown in Figure 2, all equipment using RTK was regularly blocked for several hours around the same time each day with no apparent cause. It later transpired that the source of the problem was a local amateur television transmitter mounted on a lighthouse which jammed GPS and GLONASS L2 signals with the signal shown in Figure 3. Each time the owner came home after work and switched on his system, the excavators, land surveyors and survey vessels used on the construction site lost RTK.

Figure 2: construction site at Ostend harbour

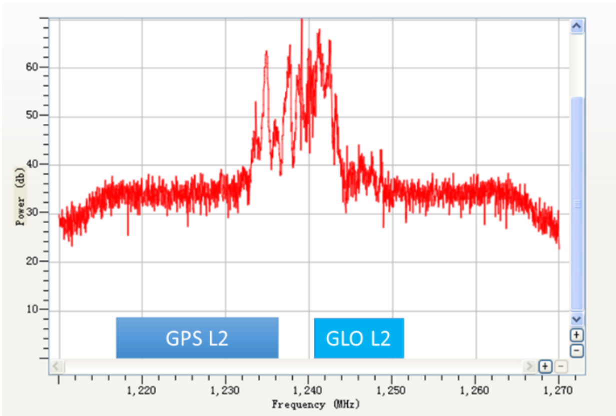

Figure 3: spectrum plot of the L2 band showing interference from an amateur television transmission

Navigation beacons

Military navigation beacons can also be problematic. These are navigation aids that transmit in the L2 band and can thus interfere with GNSS L2 signals. RTK and PPP positioning methods that require measurements from multiple frequencies can thus be rendered unworkable. Figure 4 shows the spectrum of such a system, overlapping with the GPS L2 band.

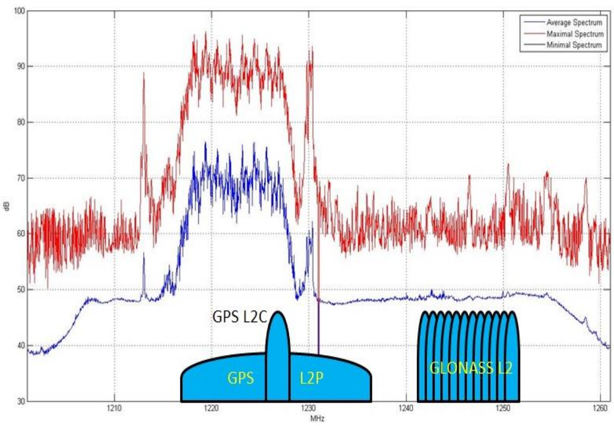

Figure 4: spectrum plot of the L2 band showing the signal from a navigation beacon in relation to the GPS and GLONASS L2 signals

Self-interference
In addition to external sources of interference, bad grounding and cabling on vessels can also produce signals disruptive to GNSS systems. Figure 5 shows the resulting L1-band spectrum when a GoPro video camera was placed directly beside the GNSS antenna connected to an AsteRx4. The three peaks are exactly 24 MHz apart pointing to their being harmonics of a 24 MHz signal: the typical frequency for a MMC/SD logging interface. The effect of this interference was enough to raise the noise floor thus reducing the carrier-to-noise levels of the GNSS signals and prevent an RTK fix.

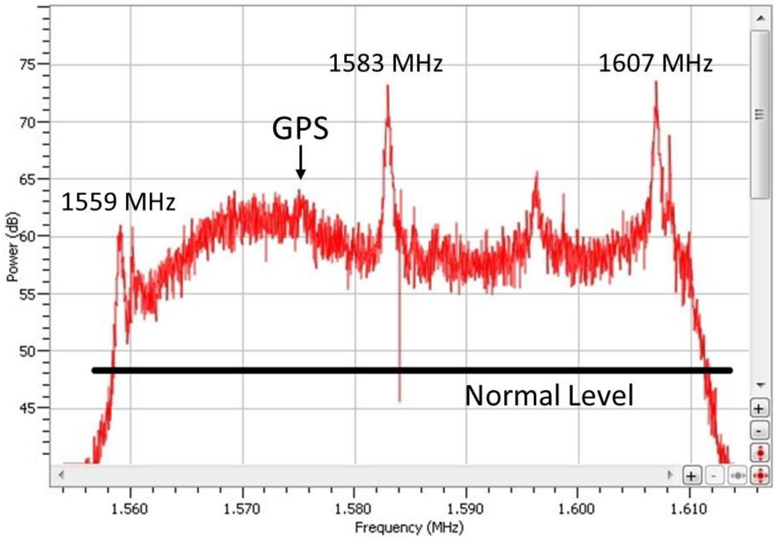

Figure 5: interference from a GoPro Hero 2 video camera picked up by a GNSS antenna

Inmarsat/Iridium uplinks
Having recently installed new satellite communication equipment on their vessels, one operator experienced outages in their GNSS positioning systems when switching on their satellite internet link. The GNSS receivers used in this case were not designed to be robust against the Inmarsat uplink transmissions in the L1 band. The choice was either precise positioning or an internet connection.
The below figure 6 shows the location of Inmarsat downlink transmission signals on the spectrum plot of the L1 band. Inmarsat uplink transmissions are located at higher frequencies and are cut by the first-stage filtering.

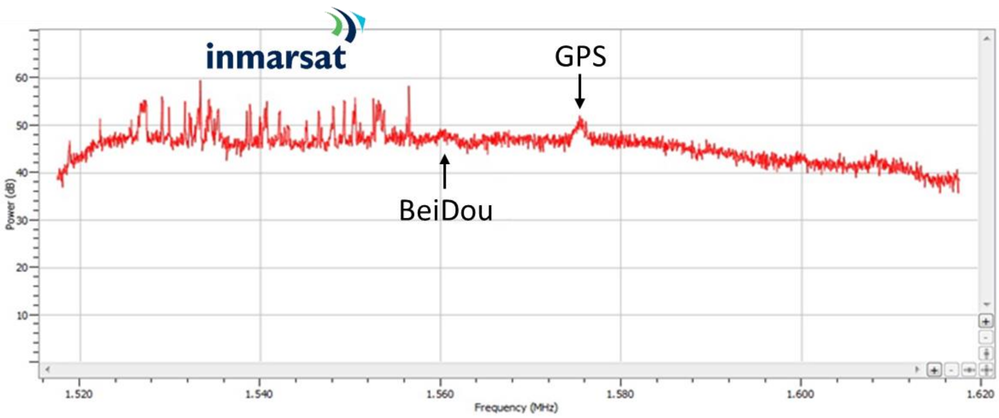

Figure 6: Inmarsat uplink transmissions are located at higher frequencies and are cut by the first-stage filtering.

Intentional jammers

Harbours are bustling with commercial vehicles whose movements are often monitored by tracking devices that include a GNSS receiver. Such devices ensure for example, that drivers don't exceed legal driving times or avoid road tolls. Recent years have seen an increase in drivers turning to cheap GNSS jamming devices, such as those shown in Figure 7, in order to move around undetected or to thwart built-in anti-theft systems.

Figure 7: typical in-car chirp jammers (PPDs (Personal Privacy Devices))

The problem is that, although these GNSS jammers or PPDs (Personal Privacy Devices) are low power, GNSS signals are even lower power. One PPD powered by a 12 V car cigarette lighter socket is powerful enough to knock out GNSS signals in a radius of several hundred meters. With the increasing use of GPS trackers for insurance or road tolling, the number of jamming incidents has increased significantly in recent years.

Most cheap, in-car PPDs transmit a chirp signal which is a signal that changes frequency rapidly over time. In this way, a signal with a rather narrow bandwidth can cover large swathes of the GNSS spectrum. Figure 8 shows the effect of a chirp jammer signal on the GPS L1 band. The region between 1565 and 1585 MHz is dominated by the jammer effectively swamping the GPS L1 signal. The time-domain signal of the chirp jammer in Figure 9 shows the characteristic frequency-sweeping behaviour. Operations in harbours (hydrographic survey, maintenance dredging etc.) may suffer unexplained loss of GNSS positioning due to such PPDs being used on vehicles operating nearby.

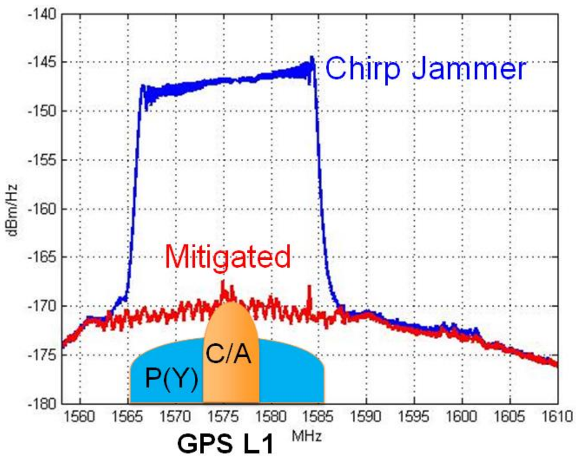

Figure 8: spectrum analyzer screenshot showing the GPS L1 signal contaminated with a chirp jammer signal both before (blue) and after (red) activation of WIMU (Wideband Interference Mitigation)

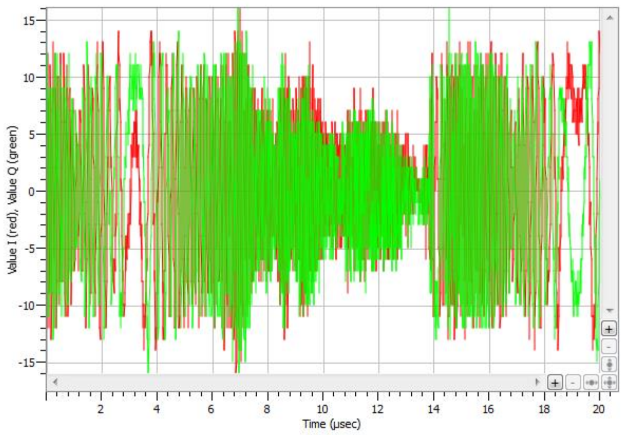

Figure 9: time-domain waveform of a typical chirp jammer

Solving GNSS interference

The previous section showed some examples of the different sources of interference that might affect GNSS signals. The interference from each of these sources is generated via a different mechanism and so each leaves their own individual footprint on the spectrum. Any approach to mitigating the effects of interference cannot therefore be one-size-fits-all: the effects of wide and narrow-band, jamming as well as continuous and pulsed interference have to be considered.

The spectrum plots and results presented in this paper, with the exception of Figure 6, use Septentrio's AsteRx4 multi-frequency RTK/PPP receiver module. This board supports all L1, L2 and E5/L5 signals from all constellations and is specifically designed for operation in harsh interference environments.

Visualisation

After down conversion with sharp Surface Acoustic Wave (SAW) filters to reject out-of-band interference, the antenna signals are immediately quantized. The raw RF signals are thus made available for either real-time visualisation using the web interface of the receiver, or can be logged for offline analysis. The logged samples can be used to detect and analyse signal anomalies in both the time and frequency domains. Armed with this information, spectral traces similar to those shown in Figure 8 and Figure 9, can immediately be identified as originating from a chirp jammer.

Mitigation

The digitized signals are automatically cleansed of interference using multiple adaptive band-stop filters. Depending on the nature of the interference, the stop-band bandwidth is adjusted automatically between a notch of a few kHz to 1 MHz-wide rejection. The notch filters are complemented by an adaptive filter capable of rejecting more complex types of interference such as that from chirp jammers and frequency-hopping signals from DME/TACAN devices. The receiver also supports regular blanking.

This multi-stage approach employing different mitigation mechanisms at the various signal processing stages allows the AsteRx4 to be robust against the largest variety of interferers. As well as offering protection against simple, continuous narrow-band interference, this interference mitigation system, also protects against high-powered Inmarsat and more complex wideband and pulsed transmitters.

Conclusion

Interference of GNSS signals as this paper has shown, can result from a myriad of sources, many of which appear at first sight to be rather innocuous. In the case of the chirp jammer – who knew that 10mW could wreak such havoc? Reported cases of GNSS interference have increased rapidly over the last few years, a trend that shows no sign of abating. The varied nature of interference signals highlights the fact that there is no single solution to the problem of interference. Further, the fact that as electronic devices continue to evolve so we can expect GNSS interference signals to become similarly more complex in character.

Interference has long passed the stage where it could be solved by antenna filters. As this paper has also shown, to combat the effects of interference, interference considerations have to be at the forefront of receiver design and incorporated into every stage of signal processing. This philosophy steered the development of the AsteRx4 receiver board. With built-in protection against intentional and unintentional jamming based on a sophisticated system of sampling and mitigation mechanisms, the AsteRx4 can suppress the widest variety of interferers: from simple continuous narrow-band signals to the more complex wideband, pulsed and high-powered Inmarsat transmitters.

Since 2006, protection against interference has underpinned receiver hardware and software development at Septentrio establishing it as the benchmark for interference mitigation in GNSS receivers.

For more information about Septentrio products and services go to septentrio.com