GNSS HARDENING AGAINST INTERFERENCE

By Dr Nick Ward & George Shaw

General Lighthouse Authorities (GLA),

Great Britain and Ireland; Research & Radio Navigation

This article was first published in the Trinity House Service journal FLASH© and appears here by kind permission of the authors and Editor

Furthermore, the article is based on a study carried out for the General Lighthouse Authorities of Great Britain and Ireland by the University of Nottingham, England, the results of which were first presented at the European Navigation Conference in Vienna, April 2013. The article concentrates on the external detection and mitigation of interference, rather than the identified techniques for improving receiver robustness.

In recent years, position input for navigation across all sectors has become increasingly reliant on Global Navigation Satellite Systems (GNSS). However, GNSS is vulnerable to signal interference. Deliberate and accidental jamming can render the whole system unusable at a particular time or location, while faults affecting individual signals can also arise. Under such conditions, GNSS equipment, including systems on ships’ bridges and GNSS-enabled aids to navigation (AtoN), can produce erroneous position solutions, which are then fed to safety-related systems such as electronic charts/displays and AIS.

GNSS receivers are vulnerable to interference, due to the low received signal powers. These low signal power levels motivate the use of spread spectrum techniques. It has been shown that unintentional RF interference (RFI) is ubiquitous. In close proximity to the GNSS frequency bands, services are active for satellite communications, TV broadcasting, radar and Ultra Wide Band (UWB) applications. These services can cause out-of-band emissions, harmonics or inter-modulation products. The weak signal environment, presence of intentional and unintentional interference and the use of GNSS in critical applications argue for an impact assessment of RFI.

The majority of GNSS receiver manufacturers agree that detection and mitigation of jammers would be a desirable feature for GNSS receivers, but some are not convinced that there is currently any real immediate threat that
demands costly changes of design to implement new features, therefore regular
design practices are considered sufficient to mitigate existing interference
problems.

As for spoofing/meaconing* of GNSS signals, no commercial manufacturer was
found, at the time of this work, to have the intention to adopt even rudimentary
spoofing countermeasures. For the GNSS receiver manufacturers to implement
such mitigation techniques there would need to be Government regulation, or
widespread recognition that vulnerabilities have been catastrophically exploited.

There have been several cases over more than ten years where GNSS
interference has been detected and localized. At Moss Landing, California, in
2001, interference was caused by the preamplifier in an active TV antenna that
had unintentional transmissions in the GPS L1 band creating a GNSS-denied
area with a radius of up to 3 km. The US Coast Guard wrote an official warning
about these antennas.

A more recent incident occurred at Newark Airport, New York, in January 2010,
where one of the GBAS (ground based augmentation system) GNSS receivers
was occasionally jammed, the investigation revealed that the jamming came
from a truck on the nearby highway where a trucker had a low power GNSS
jammer.

A number of vehicle-borne jamming incidents have been detected as part of the
UK-based SENTINEL project in 2011/2012. At least one driver has been
identified and prosecuted as a result of detailed investigations following
detection by the sensors used.

Despite these successes, a concern in all of these cases across a range of
different civilian application domains, is that the interference/jamming has
either persisted or been repeated for weeks or months before a culprit could be
identified and dealt with. As GPS becomes increasingly widely relied upon for
many services, and if the expected incidence of jamming/interference increases,
the acceptability of a multi-week cycle from incident to corrective action must
be reduced.

The density of network that may be required to protect coastal shipping, and
localised strategic access to ports through the use of single node and/or
networked detectors has been considered. The availability of existing networks
(including those independent of the GLAs) has been examined in principle,
although it should be emphasised that no discussions have been held at this
stage with the organisations mentioned.

Detection of GNSS interference involves identifying the presence of potentially
disruptive interference within a non-uniform background of noise. The process
is made difficult by the very low power level of the GNSS signal itself, which lies below the ambient noise floor.

There are no established UK networks dedicated to the monitoring and detection of interference. The closest may be the research efforts under SENTINEL which are understood to currently include four monitor points, clearly appropriate for point monitoring on an experimental basis as has been done, but equally clearly inadequate as a National monitoring network.

There are some networks that are candidates to be adapted to provide such a detection function, for example Ordnance Survey of Great Britain (OSGB) has a network of Continuously Operating Reference Stations (CORS), including an “Active network” comprising about 100 stations, with inter-station spacing of about 50 km. However, it is understood that these networks presently have no interference detection functionality.

Interference mitigation, facilitated by a monitoring network, has a number of stages. Firstly, detect, locate and intervene at the source of interference and secondly alert users so that they may take action to mitigate the interference themselves.

There would be a need to standardise alert broadcasts, both to ensure correct interpretation by user equipment and to avoid adverse effects on legacy equipment, not designed to cope with alerts. Inputs such as EGNOS Integrity alerts could also be of value.

A critical question is what should the user reaction be (both in terms of equipment reactions and of user personnel reactions) if an interference alert is received? Should equipment continue to provide GPS position fixes if they appear valid? Should they be blocked? What does valid mean? If measurements are consistent with previous measurements is that adequate? Do Receiver Autonomous Integrity Monitoring (RAIM) consistency checks have a role to play? Should a warning message be provided? Should the user be permitted to overrule the equipment’s action in the event of an interference alert? Should the equipment, or the user, switch to backup mechanisms? These questions would need to be answered before a suitable monitoring and detection system could be designed.

It is noted that the GLAs have existing data communications mechanisms already available that are potentially directly applicable to provide interference alerts. These include:

DGPS Radiobeacon channel transmissions from more than a dozen sites around the UK coast that could give coverage over a wide area around the UK;
E-Loran channel transmissions from a single UK transmitter that has sufficient range to cover a wide area around the UK.
The hardening of GNSS against interference is one of the options being explored as part of the Resilient Positioning, Navigation and Timing stream in the ACCSEAS Project, under the INTERREG North Sea Region program. Other options are eLoran, additional ranging signals (R-mode) and absolute positioning by radar.

*The interception and rebroadcasting of navigation signals.*
Fig 1 Detection Network

- GPS Sensor
- eLoran Sensor
- Rb Oscillator

Data Collection → Data Reduction → Time Error Monitor → Time Data Processing → Autonomous Adaptivity

User specific parameters and thresholds → To Server

Fig 2 GAARDIAN Probe Architecture

Jamming Incident causes enough disruption that somebody notices

Suspicion is reported

Time passes

The perpetrator is detected, found, and apprehended

A “Task Force” is dispatched to investigate

Fig 3 Detection through to Intervention

The locale is monitored, looking for the interferer(s) and their source
Fig 4 OS Active Network

Central Site

Comms Link

Remote Site

Remote Site

Remote Site

• Interference Detection
• Interference Location

• M&C
• Data Collection
• Analysis of Interference
  (Lat, Lon, (h), T, duration,
  characteristics, ...)
• Prediction of Interference

Fig 5 Interference Detection, Location, Analysis & Prediction
Fig 6 Alerting Functionality

- Alert Generation (characteristics, location, ...)
- Alert Transmission
- Alert Cancellation