Military
EMBEDDED SYSTEMS
ELECTRONICALLY REPRINTED FROM NOV/DEC 2015

Navigation warfare: GNSS denied – threat and mitigation

By Neil Gerein and Peter Soar

Bombardier Suddes and Master Bombardier Wiseman, from Y Battery Royal Canadian Horse Artillery (RCHA), plan their target engagements to support the trial of a GPS anti-jammer antenna. Photo courtesy of Defence Research and Development Canada.

Deliberate jamming of Global Navigation Satellite Systems (GNSS) – including the U.S. GPS, Russia's GLONASS, China's BeiDou, and Europe's Galileo systems – is a fact. It's a problem because the best accuracy, availability, and global coverage of position, navigation, and time (PNT) data is from GNSS. Emerging technologies show promise for the future, but the good news is that techniques and solutions already exist to ensure that "friendly forces" can have reliable, robust PNT. That robustness may be achieved by multiconstellation/frequency GNSS, multisensor navigation, and anti-jam antenna systems.

Navigation warfare (NAVWAR) threat

Deliberate, intentional jamming is occurring with increasing regularity and should now be expected as a routine aspect of operations to disrupt and deceive. As with other aspects of electronic warfare (EW), attacks on PNT capabilities are often made before any "kinetic" fighting. Examples of effective jamming include recent incidents in Korea and Ukraine. Repeated jamming against GPS, allegedly from North Korea, was experienced in South Korea between August 2010 and May 2013 when many ships and aircraft reported disruptions to the received GPS signal. More recently, the Organisation for Security and Cooperation in Europe (OSCE) has reported "military-grade" GPS jamming directed against the unmanned aerial vehicles (UAVs) of its Special Monitoring Mission (SMM) in Ukraine.

Low-level, but nonetheless insidious and illegal, jamming is pervasive. So-called "personal protection devices" (PPD) are being used to disable vehicle-tracking devices to mask the use of company-owned vehicles for private purposes, or similarly to incapacitate covert trackers that a person feels may be attached to their vehicle. Worse, GNSS jammers are now being used as part of vehicle-hijacking attacks to stop an emergency report of position being made, as reported by the FBI: "… GPS tracking devices have been jammed by criminals engaged in nefarious activity including cargo theft and illicit shipping of goods." In 2014, the UK's SENTINEL Project investigated mission-critical or safety-critical services, which need to be able to "trust" GNSS signals. It found that some key sites were reporting five to ten jamming incidents daily, and that the problem is growing.

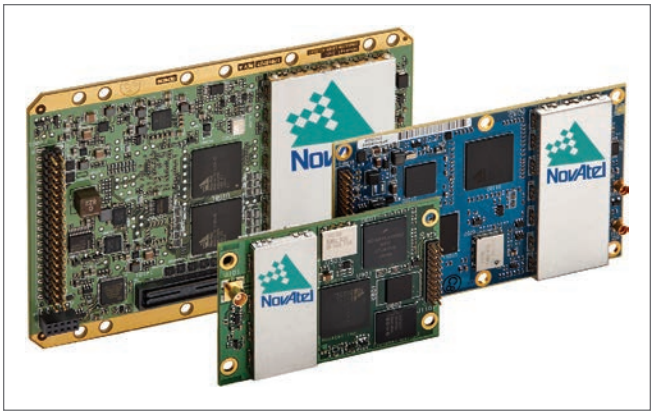

Figure 1 | OEM6 receivers feature scalable positioning options and low latency positioning with high data rates. They support all current and upcoming GPS, GLONASS, Galileo, and BeiDou satellite signals.

Despite some PPD publicity statements like "This product has low operating power and little working radius to prevent interfering with other cars or important city systems which rely on GPS navigation," some of these devices are surprisingly powerful. (Note: Readers of *Military Embedded Systems* will be familiar with the incidents in 2012 that produced harmful interference to the Ground Based Augmentation System (GBAS) at Newark Liberty International Airport.)

Spoofing is the attack method that seeks to supplant good GNSS satellite data with false signals, either by rebroadcast or by signal generation, in order to have the receiver give out incorrect position or time data. The consequences of a successful spoofing attack could be severe; consider false targeting information or the effect of taking advantage of a timing offset in high-speed financial trading. Fortunately, spoofing is much harder to achieve than the jamming discussed above if simple protection measures are used. Authorized users can take advantage of the U.S.-controlled encrypted GPS signals by using the Selective Availability Anti-Spoofing Module (SAASM) and the upcoming M-Code. The ease of capturing a normal unprotected civil receiver where its velocity is known has been demonstrated, notably by a team from the University of Texas at Austin. However, creating the same effect on a number of receivers at the same time is much harder and becomes impossible with larger numbers.

NAVWAR mitigation measures

Preventing the jamming signal from reaching the GNSS receiver is vital to interference mitigation. To this end, Controlled Reception Pattern Antenna (CRPA) anti-jam systems have proven highly effective. The CRPA and accompanying electronics dynamically change the apparent antenna gain pattern to create nulls in the direction of interference signals. This shift effectively reduces the level of interfering signal imparted on the GNSS receiver electronics. The adversary can continue to increase the jammer power until even the anti-jam antenna electronics are saturated; however, higher power jammers expose themselves to detection and geolocation techniques.

Figure 2 | The NovAtel GAJT anti-jam antenna is a single-unit GPS antenna for use on military land vehicles.

While low-power GNSS signals are susceptible to jamming, other navigation sensors can provide NAVWAR protection. Inertial sensors at present lack the long-term stability of GNSS, but they are immune to jamming and spoofing since they do not rely on radio frequency signals. Inertial sensors can be used as a consistency check against the GNSS sensor during times of attempted spoofing. They can also be relied upon during extended GNSS outages, as long as attention is given to the drift components of the inertial solution. Adding additional measurements from wheel sensors further increases resilience to jamming and spoofing.

Multifrequency GNSS receivers provide jamming protection through frequency diversity, although intentional jamming often covers all GNSS frequencies. Substantial spoofing protection is achieved by having a multifrequency/multiconstellation GNSS receiver, as simultaneous spoofing attacks against GPS, GLONASS, BeiDou, and Galileo is difficult and expensive. For authorized users, there is also the excellent option of using a SAASM-enabled receiver, which can access the encrypted signals from GPS. (Figure 1.)

"GNSS denied"

Designers, staff, and users are alert to the NAVWAR threat. As a result, the requirement for new equipment to operate in "GPS/GNSS denied" conditions is now becoming normal. It is worth drilling down beyond that statement as the denial of GNSS signals, both accidental and deliberate, can be due to a variety of reasons and the mitigation may be different for each. Therefore, it is helpful to describe the requirement. It is important to detail of the cause of the denial (e.g., blockage, jamming, spoofing), and explain the accuracy that must be maintained by the PNT system or the jamming power that it should be able to resist.

The tight coupling of GNSS + Inertial Navigation System (INS), as in NovAtel's SPAN technology, also increases system robustness against jamming and spoofing. Systems such as NovAtel's GAJT anti-jam antenna (Figure 2) protect against jamming

and add to the robustness of the PNT system. Protection from the effects of spoofing is best provided by the use of SAASM (for authorized users) although multiconstellation/frequency GNSS and anti-jam antennas also help.

The key point is that heterogeneous sensors, multiconstellation/frequency, and anti-jam protection can be used in combinations to ensure robust PNT. The correct choice of technology needs to be informed by well-defined requirements. **MES**

Neil Gerein *is the product manager, defense, for NovAtel. He joined the firm as a GPS software engineer in 2001, focusing on satellite navigation signals. In 2009 he became the defense product manager and since 2015 has been NovAtel's segment manager for defense and NAVWAR. He is responsible for the NAVWAR product lines, including the GAJT GPS anti-jam antenna and OEM625S SAASM receiver used in unmanned vehicle systems. In this role, he interacts with a wide international range of NAVWAR specialists, including Defence Research and Development Canada (DRDC). His early career was as an engineer at Vecima Networks and Navsys Corp., where he worked on beamforming GPS receivers. Neil earned an M.Sc. in Electrical Engineering at the University of Saskatchewan. Readers may reach Neil at neil.gerein@novatel.com.*

Peter Soar *is the business development manager, military and defense, for NovAtel. He was commissioned as an officer in the Royal Artillery of the British Army in 1976 and was sent to the University of Surrey to read an Honours Degree in Engineering. After graduation he rejoined his regiment and served in a variety of appointments at home and abroad including field artillery, air defense, antiterrorist, and ceremonial. Upon leaving the army in 1994, he assumed a series of roles in the City of London and subsequently joined QinetiQ as a principal project manager for Indirect Fire Rockets and Navigation Warfare (NAVWAR); he took on sales roles for NAVWAR, Autonomy, and Global Navigation Satellite Systems business lines. Peter joined NovAtel in 2012, is based in England, and reports to the corporate headquarters in Calgary, Alberta. Readers can reach Peter at peter.soar@novatel.com.*

NovAtel • www.novatel.com