NovAtel's Thought Leadership Series

INTERFERENCE & JAMMING: (Un)intended Consequences

Personal privacy devices. LightSquared. Solar max. It can be a hostile world out there for GNSS technology.

The threats just keep growing to a resource that hundreds of millions of people around the world have come to rely on for a myriad purposes.

GNSS is, after all, an RF technology, vulnerable in its own way to the kind of disruptive effects that turn an AM radio into a static-ridden howl as you drive under a powerline. And the radiated energy of signals arriving with from satellite sources tens of thousands of miles away are orders of magnitude weaker than those carrying the top 40 tunes broadcast by a local station.

Powerful terrestrial wireless broadband systems, such as the one proposed by LightSquared Inc., can overwhelm sensitive receiver elements without even transmitting signals directly into GNSS bands.

And now, intentional jamming is no longer a phenomenon limited to theaters of military operations where attacks on positioning and navigation systems accompany efforts to deny communications and electronic surveillance to the enemy. Truck drivers seeking to thwart monitoring by dispatch centers or avoid federal limits on hours behind the wheel, use low-power jammers to disable a receiver a few feet from them—with no idea that they may be interrupting GNSS-based systems miles away.

Even Mother Nature gets into the act with solar flares, scintillation, and electron-fueled ionospherics.

To help sort the signal out from the noise surrounding this subject, we turned to Phil Ward, an electrical engineer and president of Navward GPS Consulting who has worked on GPS receiver design since 1976. A senior technical staff member at Texas Instruments Defense Systems and Electronics Group for 31 years, Ward is a fellow and former president of the Institute of Navigation and a senior member of the Institute of Electrical and Electronic Engineers.

> **NovAtel's Company Values**
>
> Innovation and Integration are cornerstones of our business, we believe that excellence is the standard and we always encourage new ideas.

Categorically, what are the most common forms of interference, intended and unintended, in civil and military environments?

WARD: The most common forms of unintended interference for both civil and military environments are "in-band" harmonics of legitimate but nearby, high-powered transmitters, especially those of radars. The term "in band" should be interpreted in two ways: (1) Unwanted power spectrum that is within the specified GNSS band, in which case it will not be attenuated by the receiver front-end bandpass filters. (2) Unwanted power spectrum that is outside the specified GNSS band, in which case it will be attenuated by the receiver front-end bandpass filters, but can result in interference because the arrival power level is so high that it overcomes the front-end filter attenuation. The first interpretation is the usual one for "in-band" interference, but the second is also effectively "in-band" interference and can best be illustrated by the recent LightSquared fiasco.

As for the most common forms of intended military interference, all military GPS receivers need to mitigate every form of jammer, including pulsed, matched-spectrum, band-limited white noise (BLWN), and other wideband jammers as well as continuous wave (CW) and the numerous variations of narrowband jammers.

Which forms of interference/jamming are most serious from the point of view of the relative difficulty in mitigating their effects?

WARD: Matched-spectrum and BLWN wideband interference/jamming are the most difficult forms to mitigate because, only advanced antenna technology (such as a controlled reception pattern antenna) can further improve any other receiver enhancements against this threat. Matched-spectrum jammers are more complex to design, but are typically 1.5 times more effective than BLWN jammers (for the same null-to-null transmitter power levels). CW and other narrowband (NB) jammers are typically two times more effective than BLWN jammers for the same transmitter power level but they are also the easiest to mitigate (by various forms of spectral excision). Because no such mitigation exists in civil GPS receiv-

ers, the current "GPS privacy jammers" use NB techniques effectively.

Which elements of a GNSS receiver are affected by interference/jamming and which are the most vulnerable to its effects?

WARD: The GNSS receiver analog front-end, usually called the integrated front-end (IFE), is the typical weak link when it comes to interference/jamming in civil GNSS receivers. If the IFE (including its automatic gain control) does not instantly recover from each pulse in the presence of pulse interference/jamming, then the significant portion of time that the GNSS signal is present after each pulse has ended cannot be tracked by the downstream digital signal processing.

If the IFE does not possess a very high dynamic range (including the use of precisely controlled attenuators as the interference/jamming levels increase), then the IFE quickly goes into gain compression that prevents any meaningful downstream digital signal processing against all forms of wideband and narrowband jammers. If the IFE has no designed-in means of spectral excision, then narrowband interference/jamming is typically two times more effective than BLWN interference/jamming for the same amount of in-band power.

Assuming that all of the IFE design techniques have been applied, then ultimately the interference/jamming creates excessive jitter in the receiver code and carrier tracking loops, causing them to lose the ability to track the SV code and carrier signals, respectively. The carrier-tracking loop is by far the most vulnerable.

What seem to be the most promising avenues of countering interference and jamming in 1) receiver/antenna designs, 2) other RF or sensor technologies, and 3) external sources of aiding?

WARD: In the context of military navigation and timing technology, the most promising avenue is in antenna and IFE designs using n-element controlled reception pattern antennas (CRPAs) and "n" matched IFEs. A CRPA steers the antenna gain nulls in the direction(s) of the jammer(s) and a small amount of gain toward the space vehicles (SVs). An even more expensive antenna technology is a multiple-beam phased-array antenna with each high-gain beam pointed toward one SV resulting in much lower gain towards the jammer(s), unless co-located in direction.

Any other RF technology will also be vulnerable to interference and jamming, but the most robust RF technology as a position and timing backup to GNSS for civil users is the ground-based, two-dimensional eLoran system as the successor to the legacy Loran C system. Like Loran-C, the eLoran system transmits a very powerful signal with a very long wavelength requiring potential jammers to use extremely large antennas and enormous jamming power to be effective. Unfortunately, this is no longer "the most promising" because the entire U.S. Loran-C system was cancelled by Executive Order in 2009, without mention of the proven and partially operational eLoran system.

The best external source for GNSS velocity aiding is an inertial measurement unit (IMU). As is well known, IMUs are unaffected by interference/jamming; however, they also "drift," while GNSS is vulnerable to interference/jamming but does not drift. So, integrated GNSS/IMU technology will always be a highly synergistic combination because the IMU not only provides excellent velocity aiding but also provides navigation holdover when the GNSS system can no longer operate in the presence of interference/jamming. Doppler radar (with a gyroscope to provide heading) also has been used for velocity aiding but it is not as accurate as an equal cost IMU, and it is vulnerable to jamming. IG

Phil Ward,
Navward GPS Consulting

> "**Any other RF technology** will also be vulnerable to interference and jamming, **but the most robust** RF technology **as a position and timing backup to GNSS** for civil users is the ground-based, two-dimensional **eLoran system.**"