

GPS in networked systems ..part 1

Dr Carlo Kopp

NCW 101 Part 12

The Navstar Global Positioning System (GPS) is now ubiquitous, and is playing an increasingly important role in modern networked warfare. Applications range from navigation, GPS aided network traffic routing through to weapon guidance.

GPS had a long gestation period, with initial conceptual development work performed during the early 1960s, and full scale operational use not happening until the 1990s (refer Milestones 'Stellar navigation to Satellite navigation' March/April issue p60). Since then GPS has emerged in a vast range of applications, importantly these spanning man-portable systems up to major capital warships.

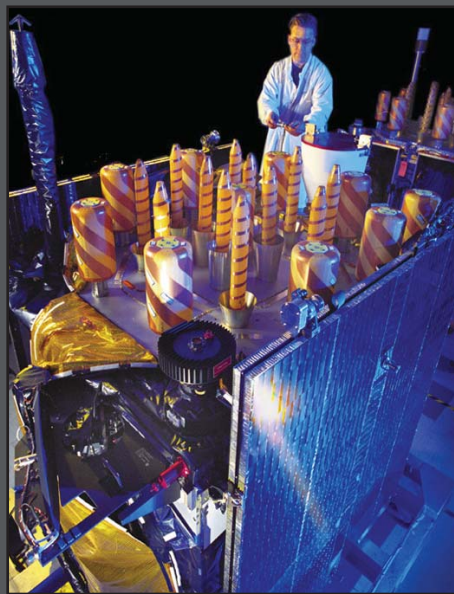
What GPS and its Russian Glonass and European Galileo siblings provide is low cost all-weather navigation position fixes with good accuracy – and in newer differential systems, high accuracy. With GPS becoming widely used in commercial applications, the cost of many GPS chipsets has declined to the trivial. This trend will continue as GPS appears more frequently in mobile phones, laptops and other portable devices.

The ubiquity of GPS and its low cost have resulted in its progressive integration into a wide range of systems, resulting typically in capability gains but also in an increasingly systemic dependency on the availability of GPS. If GPS is impaired, some systems may become unusable, and others reduce in capability or accuracy. The technological marvel that GPS may be is nevertheless a double-edged sword, through the dependency and susceptibility it introduces.

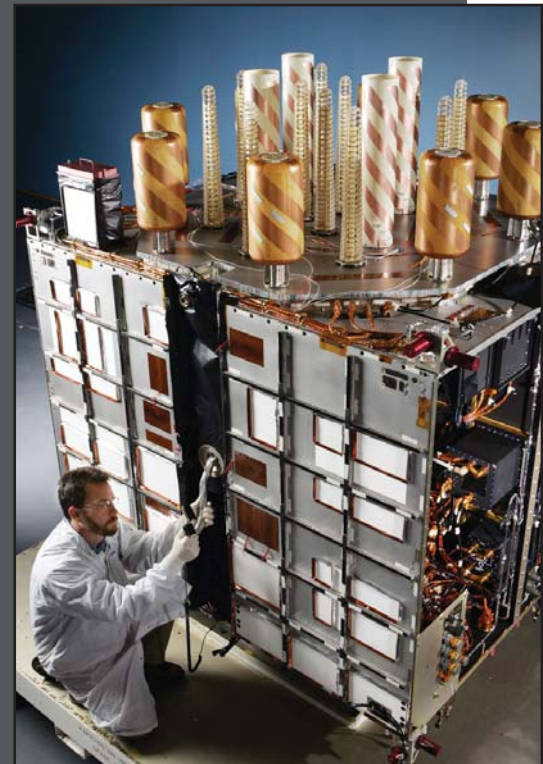
Jamming

Jamming by technologically competent hostiles was and will remain an issue for all satellite navigation systems. The low power level radiated by the Block II series satellites introduces vulnerability to both interference and jamming. The power level to be detected by a GPS receiver is -160 dBm (decibel-watts wrt one milliwatt, or 10⁻¹⁹ Watts), which is by typical broadcast radio standards miniscule. It is intended that Block III SVs will have the capability to focus 'spot beams' of higher power output on areas of interest precisely to reduce this problem.

In practice, this vulnerability was first observed in some parts of the US where GPS signals were jammed by harmonic interference from commercial TV stations operating in the VHF band plus mobile



The latest Block IIR-M satellites add a civil L2C carrier and military M-code.



telephone transceiver towers operating in the UHF band. Even the small amounts of energy leaking from these transmissions into the 1.5 GHz band were found to produce volumes of space, miles across, where airborne GPS receivers were unable to maintain lock and dropped out.

For military operations this vulnerability remains a major concern. Even low powered jammers radiating pseudo-noise signals against the GPS carriers could cause typical receivers to either break lock or fail to acquire satellites from distances of tens of miles. A one Watt transmitter (comparable to a mobile phone) at a distance of 60 km (32 NMI) can in theory prevent a common GPS receiver from acquiring the C/A code. Military receivers locked on to the encrypted P(Y) code are more resilient and around 100 W of jam power at 20 km (10.7 NMI) is required to break lock. A jammer radiating hundreds of Watts can foil satellite C/A code acquisition at ranges of several hundred nautical miles. A hostile party could potentially disrupt many early generation receivers

by the simple expedient of hoisting such jammers to several thousand feet altitude on devices as simple as tethered balloons.

Numerous Electronic Counter CounterMeasures (ECCM) have been used to improve the resilience of GPS receivers to jamming. The first technique was the use of Controlled Reception Pattern Antennas (CRPA), which can electronically form antenna beams in the direction of satellites, thereby boosting the signal relative to the jammer signal. This typically improves Signal/Jammer power ratios by 30 dB (1000 fold).

Additional improvement can be achieved by adding a Nuller to the receiver antenna. A Nuller will suppress antenna sensitivity in the direction of a detected jammer, and this together with CRPA beamforming techniques provides a 50 dB improvement in resilience against jamming. If the receiver is locked-on to the P(Y) PPS code, and uses these techniques, jamming power levels of hundreds of kiloWatts at several miles of distances will be required to break lock.

It is worth observing that attempts by Saddam's regime in 2003 to disrupt JDAM attacks using imported Russian jammers led to the destruction of the jammers by JDAM attack.

The greatest risk with jamming will not arise with receivers fitted to platforms or expensive smart munitions, but primarily with low cost man portable or vehicular equipment, where economics preclude the addition of a complex electronically steerable antenna and associated processing hardware.

GPS in Network Centric Warfare

In a networked environment, GPS provides a number of valuable capabilities, many of which are yet to be fully exploited. The first is that GPS provides a completely unified coordinate system and thus positional frame of reference for all users. This means in practical terms that positional data can be exchanged transparently by all users without fear of errors arising from different mapping schemes.

The second benefit is that GPS provides an accurate shared timebase across all user systems. This is especially valuable in multi-static systems where sensor data is fused from a wide range of systems in physically different locations. For instance, tagging hostile radio or radar emissions with directional, positional and timing data can much improve confidence levels in threat identification and later targeting.

The third benefit is a byproduct of the previous two, in that location information on friendly systems is consistent in relative terms, with known errors facilitating deconfliction and friendly fire avoidance. The fourth benefit is least obvious, which is Location Aided Routing in ad hoc or self-forming network protocols. Knowing where a friendly platform is located permits a smart networking protocol to make clever choices about where and how it routes network traffic.

Inside The GPS System

While the inner workings of GPS have been widely discussed, this is less so the case with its military modes and associated capabilities. To appreciate their importance, it is worth taking a close look at the GPS system.

The GPS network has three key components – the orbital constellation, the supporting ground stations, and the user terminal equipment.

The GPS orbital constellation currently comprises no less than 30 Block II/IIA/IIR/IIR-M satellite vehicles, with the first operational Block II SV was launched in February 1989. These SVs are in 10,988 nautical mile inclined 12-hour polar orbits, arranged such that most of the globe is covered at any time by a sufficient number of satellites to provide a viable navigational fix. At any time 24 are active, with the remainder on standby as spares.

Rockwell International produced the Block II/IIA SVs (13 through 21 and 22 through 40) designed to last seven years in orbit. These are now being progressively replaced with the Block IIR/IIR-M 'replenishment' SVs produced by Lockheed-Martin (41 through 62). The Block IIF SVs due for first launch this year follow the Block IIR-Ms.

The Block II/IIA/IIR SVs transmit a continuous spread spectrum radio signal, with time-synchronised codes designed for accurate ranging on two carrier frequencies, L1 and L2 at 1575.42 MHz and 1227.6 MHz respectively. Also transmitted is a continuous stream of encoded supporting data, the Navigation Message, divided into multiple frames or pages.

Both the L1 and L2 carriers are modulated in phase (conceptually similar to FM radio) with Pseudo-Random Noise (PRN) codes. The C/A (Coarse/Acquisition) code is a 1023 bit 1 MHz PRN code which is unique for each satellite, and is used by military receivers to acquire and lock-on to the P-code, whilst in civilian receivers it is the

navigational reference signal. The military P-code is a seven-day repetition cycle 10 MHz PRN modulation, which is imposed upon both the L1 and L2 carriers. It is usually encrypted to P(Y) code, and can only be used if the user has both a military GPS receiver as well as the classified crypto key to decode it with. The P-code modulation on the L2 carrier is used by military PPS receivers to measure ionospheric transmission delays. The third code, the Navigation Message, is a 50 bits/s digital signal, which contains six-second duration frames comprised of five 300 bit subframes of data.

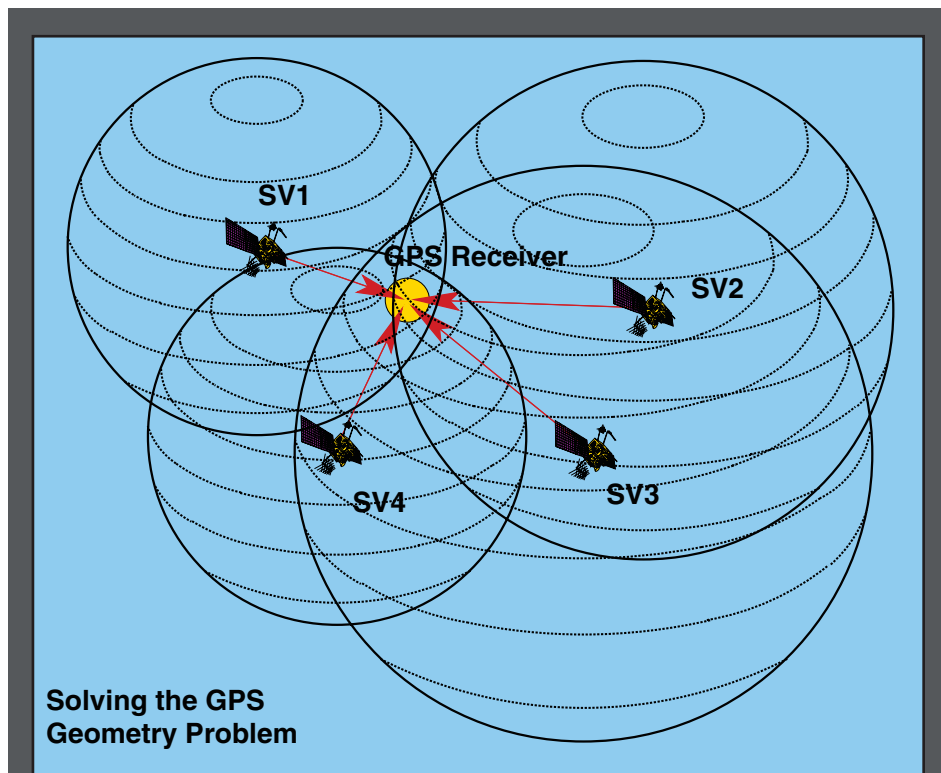
The latest Block IIR-M SVs also transmit an additional L2C (civil) carrier at the L2 frequency, used to enhance accuracy of commercial equipment, along with an additional military M-code added to improve jam resistance. The follow-on Block IIF SVs will add a third civil carrier, L5, at 1176.45 MHz.

The Navigation Message is broadcast by each satellite. It contains encoded clock corrections, precise orbital data, correction parameters for an ionospheric model, and Almanacs, which describe approximate satellite orbital data over extended periods of time. The latter are used to cue the receiver to which SVs are above the horizon and thus potentially visible.

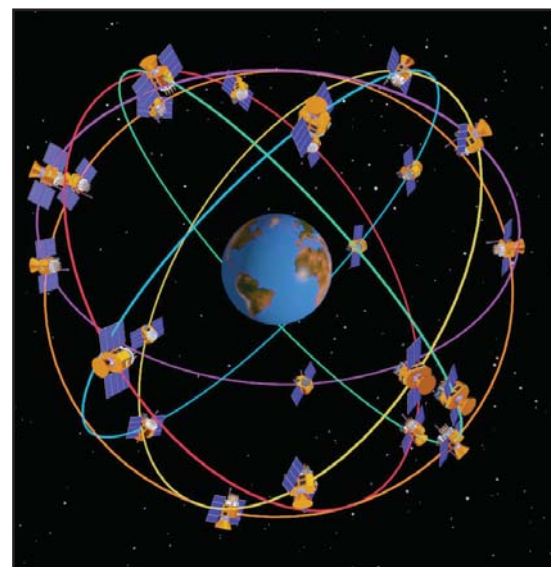
A GPS receiver will extract this data from the NM signal, and use it to correct its clock to within 100 (PPS) or 167 (SPS) nanoseconds of UTC (GMT) time, as well as to calibrate its internal model for the satellite orbit, and its internal model for ionospheric delays.

The C/A and P-codes are then used for measuring 'Pseudo-Range' to each respective satellite. A receiver will use an internal PRN code generator to produce a PRN code for each of the satellites. This code is then compared to the received satellite signals using a circuit termed a 'correlator', and if the PRN codes match the receiver can lock-on to the satellite to perform a 'Pseudo-Range' measurement.

When a receiver's PRN code generator is in lockstep with the satellite's transmitted PRN code the time at which the repeating PRN code starts is extracted. This time is termed the Time Of Arrival (TOA) and the difference between the TOA and receiver internal time, adjusted for the offset between receiver time and GPS network time, is a measure of the distance to the satellite. The range thus calculated is termed Pseudo-Range.



The Pseudo-Range measurements produced by a receiver represent spheres of constant distance around each satellite. With multiple satellites this allows the position of a point common to all spheres to be computed, which is the location of the receiver (Author).



GPS constellation.

A GPS receiver will then use the four or more Pseudo-Range measurements to compute position in Earth-Centred, Earth-Fixed (ECEF XYZ) coordinates. These are then converted by the receiver into geodetic latitude, longitude and height above the surface of a rotational ellipsoid, typically using the WGS-84 Earth model, although other models may be used. As the GPS system assumes the WGS-84 model, use of other models without correction can produce significant positioning errors.

GPS receivers can measure platform velocity by differencing consecutive position measurements, or by measuring the Doppler shift of satellite carrier signals and using this with computed direction to each satellite, to calculate velocity in three axes. Conceptually, this is like an 'inside out' Doppler Navigation system. Some receivers may use both methods to improve accuracy.

All of this complexity is buried inside SVs and the receiver chipset usually supplemented by a microprocessor chip, which performs supporting tasks and generates formatted navigation data output to the other components of the system.

GPS navigation receivers are now cheap, mostly due to the high density of current chip technology, which allows nearly all of the hardware to be embedded into a single chip or small number of chips.

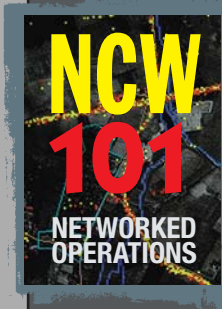
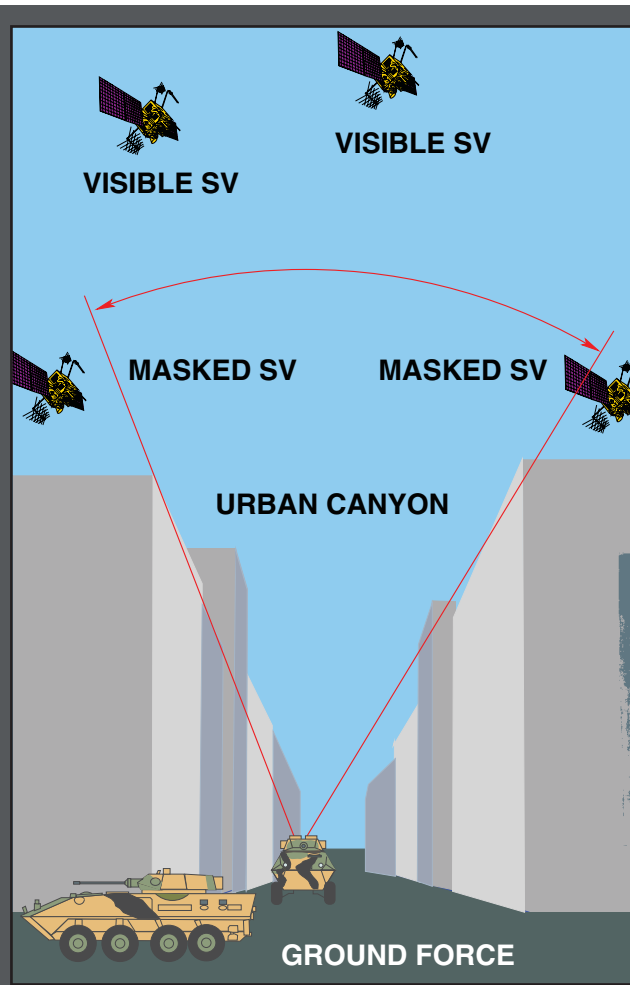
The usual measure of quality in a GPS receiver is the number of channels it uses, each of these being an independent receiver and decoder/correlator path. A single channel receiver, typical in first generation GPS equipment, is slow since it has to consecutively step through each of the visible satellites to perform an NM download and Pseudo-Range measurement. For military applications, especially guided weapons and fast platforms like aircraft, this was inadequate and soon led to multichannel receivers, mostly five channel devices, although eight channel receivers also exist.

GPS Errors

GPS, like all navigational schemes, has a range of inherent sources of navigational error. Electrical noise in the receiver, as well as phase noise in the PRN code modulation will typically degrade accuracy by about two metres. Each Block II/IIA SV uses four atomic clocks (two cesium and two rubidium), the Block IIR/IIR-M SV uses three rubidium atomic clocks. These are highly accurate but nevertheless drift in time.

If satellite clock errors are not corrected by the ground station this will degrade accuracy by about one metre, over time. Errors in orbital position estimation will also lose about one metre.

Another error source is unmodelled signal propagation delays in the troposphere due to changes in humidity, temperature and pressure changing the refractive index, which will lose about one metre. Multipath propagation, the effect of



The Urban Canyon problem – tall obstacles mask SVs causing dropouts or GDOP problems.

satellite signals bouncing off obstacles and arriving from several directions each with different time delays, can further degrade accuracy by about 0.5 metre.

The biggest single natural source of error is, however, unmodelled ionospheric signal delay, as the model broadcast by the satellites can only compensate for about one half of the possible error, with the resulting error being up to 10 metres.

Another effect comes into play: Geometrical Dilution Of Precision (GDOP) where the angles to the satellites in view are very similar, GDOP will result in inaccuracy in solving the coordinate equation, which will further degrade the resulting navigational solution.

A problem related to GDOP is that of complex or 'urban canyon' terrain, where a receiver can 'see' only a small number of satellites due to tall surrounding obstacles. The result is often a loss of navigational solution or a large GDOP error. This is termed the 'Mask Angle Problem', and to achieve a 15 degree Mask Angle a constellation with 30 to 36 active satellites would be needed, increasing the cost of the orbital segment by up to 50 per cent.

As all of these sources of error will fluctuate in time, users may experience substantially better accuracy at some times, and worse accuracy at other times, depending on the geometry of the satellites in view and ionospheric conditions. Non-military users historically experienced an artificially produced error, resulting from Selective Availability (SA) until it was disabled some years ago. The SA mechanism introduces a time varying bias in the C/A signal, which is designed such that it is virtually impossible to remove. The potential C/A code accuracy of at least 30 metres is thus reduced to the nominal 100 metres.

GPS has provided accuracy and a universal positioning system for use in a multitude of technologies, including those for military purposes where response time and accuracy is critical.

Part 2 of "GPS in networked systems" will further discuss NCW benefits derived from GPS, and also explore differential GPS in its various forms.