# Iraq and GPS: Some Frequently Asked Questions

Richard B. Langley
Dept. of Geodesy and Geomatics Engineering
University of New Brunswick
<lang@unb.ca>

13 March 2003

## 1. If a war starts with Iraq, will GPS be turned off or will there be a global reduction in available accuracy?

Prior to 2 May 2000, the accuracy afforded users of the GPS Standard Positioning Service (SPS) was purposefully degraded through a policy and technique known as Selective Availability (SA). The use of SA gave military users of GPS a position accuracy advantage – one it did not wish to share with potential adversaries. SA was effected by manipulating or dithering the output of each GPS satellite's active atomic clock. This clock controls the generation of all of the satellite's signals and hence the measurements made by a GPS receiver. SA was imposed at a level which would yield a stated SPS horizontal (latitude and longitude) accuracy of 100 metres or better 95 percent of the time for any point in the world during a measurement interval of one day. On 2 May 2000, by presidential decree, the level of SA was set to zero. SPS users immediately saw a quantum jump in positioning accuracy with factors of 5 to 10 improvements. Even a simple handheld receiver can now often yield horizontal position accuracies of 5 metres.

When SA was set to zero, the United States Government stated that it had no intent to ever use SA again. According to the Interagency GPS Executive Board, the U.S. government agency that manages GPS, there has been no change in this policy. The decision to effectively switch off SA came four years after the adoption of a government policy document which stated, in part, that it was the government's intention "to discontinue the use of GPS Selective Availability (SA) within a decade in a manner that allows adequate time and resources for our military forces to prepare fully for operations without SA." Basically, this meant that the military would develop measures to prevent the hostile use of GPS to ensure that the U.S. retains a military advantage. But it was to do this in a manner which would not unduly disrupt or degrade civil use of GPS. The number of civil GPS users far exceeds the number of military users and is estimated to be in the tens of millions worldwide. Civil GPS uses include the navigation of commercial

aircraft, oil tankers, trucks, and space vehicles. Many emergency service providers now rely on GPS to more quickly respond to accidents.

The technique the U.S. military developed which allowed them to switch off SA is selective in-theatre jamming of the SPS signal.

So, if there is a war with Iraq, it is highly unlikely that SA would be re-imposed as it would affect all civil GPS users worldwide. It is also highly improbable that GPS signals would be simply switched off.

**2. Will the U.S. jam GPS in Iraq?**

The U.S. military certainly has the capability to jam the GPS SPS signal using either ground-based jammers or jamming transmitters onboard aircraft. Extensive jamming tests have taken place on military reservations in the U.S. over the past decade. But would the U.S. actually use jammers in Iraq?

To answer this question, we must know something about the GPS signals and how they are used by civil and military receivers. The SPS uses the C/A-code component of the GPS L1 signal which is transmitted on 1575.42 MHz. The C/A-code, which stands for coarse/acquisition-code, is a pseudorandom noise code which the GPS receiver uses to determine the distance to a satellite. The distance is determined by aligning the received code with a replica of the code generated in the receiver. By measuring at least four such distances to different satellites simultaneously and knowing where the satellites are from the navigation messages they transmit, the receiver can figure out where it is. The C/A-code is a relatively short code which repeats every millisecond and a GPS receiver can easily lock onto or acquire it.

The military's GPS capability is known as the Precise Positioning Service (PPS). It relies on a much longer code called the P-code (for precise or precision) which is transmitted on both the L1 frequency and the L2 frequency at 1227.60 MHz. The P-code is encrypted (and it's then called the Y-code) so that it cannot be accessed by unauthorized users. Encryption also prevents a military GPS receiver from being fooled or spoofed by a fake GPS signal transmitted by an enemy. The encryption process is known as Anti-Spoofing. Military GPS receivers have decryption capabilities which permit them to recover the P-code.

Each satellite's unique P-code segment is one week long. In order to determine the distance to a satellite using the P-code, the receiver must align a replica of the code it generates with the arriving code. With such a long code, it was formerly difficult for the signal processors in P-code receivers to quickly find the correct alignment point in the code without help. It got this help from the C/A-code. So even though military GPS receivers determine their position (and velocity and time) from the P(Y)-code, they generally have acquired the C/A-code first and then using information from that signal have zeroed in on the P-code. Most of the military-grade GPS receivers now in existence work on this principle.

Advances in receiver technology now permit direct acquisition of the P-code without relying on the C/A-code. This new technology has been combined with improved security procedures to prevent the use of military GPS receivers by unauthorized personnel. GPS receivers with this capability include a module known as SAASM (Selective Availability Anti-Spoofing Module). All new receivers acquired by the military after 30 September 2002 are to include the SAASM. According to its Web site, the GPS Joint Program Office had authorized over 2,050 procurements of SAASMs and SAASM-equipped devices as of 22 October 2002. Although some older receivers can be retrofitted with the SAASM technology, the Defense Department has not mandated such action.

So, to get back to the question: "Will the U.S. jam GPS in Iraq" – they certainly have the technology to do so. The C/A-code can be selectively jammed without significantly affecting reception of the P(Y)-code. SPS receivers would then become useless. However, as we discussed, most military GPS receivers now in the field use the C/A-code before switching to the P-code. Operation of these receivers would be made difficult in the presence of C/A-code jammers. It might be possible to initialize a receiver outside the range of a jammer so that it is already operating on the P(Y)-code once it gets inside the jammer's coverage zone. However, should it temporarily lose lock on the satellite signals, the receiver might have difficulty in reacquiring them.

Some military GPS receivers come equipped with anti-jam technology, such as null-steering antennas, and these receivers could continue to operate in the presence of a jamming signal.

So, the U.S. military may or may not jam GPS in Iraq. The decision to do so will depend on whether or not they think the Iraqis are using GPS (would you really want to rely on your enemy's system?) and whether or not its use would compromise their own operations.

**3. Will the Iraqi military jam GPS?**

It is relatively easy to build a GPS jammer. One can be built from a surplus direct-to-home satellite TV receiver or from scratch using plans which can be found on the Web. A company in Russia actually markets GPS jammers and it has been reported that the Iraqis have purchased some of them. So, the Iraqi military might try to use GPS jammers in an attempt to foil GPS-equipped weapons such as the Joint Direct Attack Munition (JDAM). But, such actions would likely not be successful. In the first place, JDAMs include an inertial navigation system which would continue to navigate the bomb should its reception of GPS signals be disrupted. And, like any radio transmitter, the location of a jammer could be easily found and the device neutralized.

**4. Where can I learn more about GPS and its military uses and jamming and anti-jamming technologies?**

*The Precision Revolution: GPS and the Future of Aerial Warfare* by Michael Russell Rip and James M. Hasik, published by the Naval Institute Press, Annapolis, Maryland in 2002.

"Satellite-Guided Munitions," by Michael Puttré in *Scientific American*, Vol. 288, No. 2, February 2003, pp. 66-73.

"Jamming GPS: Susceptibility of Some Civil GPS Receivers," by Börje Forssell and Trond Birger Olsen in *GPS World*, Vol. 14, No. 1, January 2003, pp. 54-58; <http://www.gpsworld.com/gpsworld/article/articleDetail.jsp?id=43432>.

*Global Positioning System: Signals, Measurements, and Performance* by Pratap Misra and Per Enge, published by Ganga-Jamuna Press, Lincoln, Massachusetts in 2001.