Jamming GPS

Susceptibility of Some Civil GPS Receivers

Börje Forssell Norwegian University of Science and Technology
Trond Birger Olsen Norwegian Defence Logistics Organization

How susceptible are Standard Positioning Service GPS receivers to different kinds of jamming? The U.S. Department of Defense will use in-theatre jamming of the L1 signal to deny its adversaries the use of GPS. While jamming GPS signals has always been a military option, its use became a necessity following deactivation of Selective Availability. In addition to such military procedures, terrorists might try to jam the GPS signals using easily constructed equipment. GPS signals are also susceptible to unintentional jamming from neighboring users of the radio spectrum.

Jamming signals can take different forms, and just how a receiver responds to a jamming signal depends on several factors. In this month's column, two Norwegian authors describe the influence of different types of jamming signals on the ability of L1 C/A-code GPS receivers to acquire and track satellites under various circumstances and they report the results of testing three different receiver types using an advanced GPS simulator system.

Dr. Börje Forssell *is a professor and former head of the Department of Telecommunications of the Norwegian University of Science and Technology in Trondheim. He has been a visiting scientist at several European institutes and has been a guest professor at the Tokyo University of Mercantile Marine. For the 2002-03 academic year, Dr. Forssell is a visiting scientist at the European Space Agency's European Space Research and Technology Centre in Noordwijk, The Netherlands, taking part in the development of Galileo. He is a member of the Editorial Advisory Council of Galileo's World and a fellow of the Royal Institute of Navigation.*

Lt. Trond Birger Olsen *is an avionics officer at the Norwegian Defence Logistics Organization/Air in Kjeller specializing in electronic warfare systems. He has attended the Norwegian Air Force Training Establishment in Kjevik, the Air War College in Trondheim, and the Norwegian University of Science and Technology.*

The vulnerability of civil GPS receivers has long been known, but it has rarely been taken into account by receiver manufacturers or users. Only some five years ago, when the U.S. Department of Defense started comprehensive activities related to GPS and warfare (navigation warfare or NAVWAR for short), did it become publicly clear that jamming of civil receivers should be taken as a serious issue.

The definition of NAVWAR reads: "an environment in which

- friendly forces maintain their ability to use satellite navigation,
- satellite navigation is denied to hostile users,
- there is no effect upon civilian applications."

This definition makes it clear that the issue includes more than protection of the military's own receivers.

The civil GPS community got an eye-opener in 1997 as well. First, the Russian company Aviconversias announced in September that it could deliver a commercial GPS/GLONASS jammer capable of blocking civil GPS receivers within a radius of 200 kilometers. Then, military GPS testing in the New York area in December caused a number of GPS receivers in civil aircraft to lose track of GPS signals during approach into Newark International Airport. Thus, it was confirmed that civil receivers were vulnerable to jamming, and at the same time, that jamming equipment was commercially available.

As a consequence of these and other events, several analyses of the vulnerability of GPS-based transport systems have been carried out. One of the most important studies in this field, and — coincidentally — with very good timing, was the so-called Volpe report on the vulnerability of GPS which concluded that, like other radionavigation systems, GPS is vulnerable to jamming, and that jamming of GPS could jeopardize safety and have serious environmental and economic consequences. The report also concluded that increased use of GPS in civil infrastructure makes it an increasingly attractive target for hostile activities by individuals, groups and states. At the same time, the analyses underlined the commercial availability of equipment for jamming purposes.

Our Research Goals

The purpose of the work described in this article was to investigate how civil GPS C/A-code receivers react to certain types of interfering signals. It should be remembered that, after all, most interference with GPS signals is unintentional, coming from transmitters established for other purposes. For this reason, we investigated certain generic classes of interference.

We wanted to answer the following questions:

- What signal types are most "efficient" as interferers/jammers?
- How does a GPS receiver react to different interference power levels?
- Can receiver responses be theoretically predicted with high reliabilty?

The efficiency of interfering signals is defined with regard to the relationship between interference level and loss or unacceptable reduction of navigation ability by the receiver as well as loss of its capability to regain normal navigation performance when the interference stops.

Thus, the most efficient interfering signal is one which needs the lowest power level to make the receiver lose navigation ability and at the same time prevents the receiver from regaining that ability.

Equipment

The interfering signals were generated by a commercial interference generator connected to a GPS signal simulator. The generator output signal, that is, a combined RF signal consisting of simulated GPS signals plus interference, was used

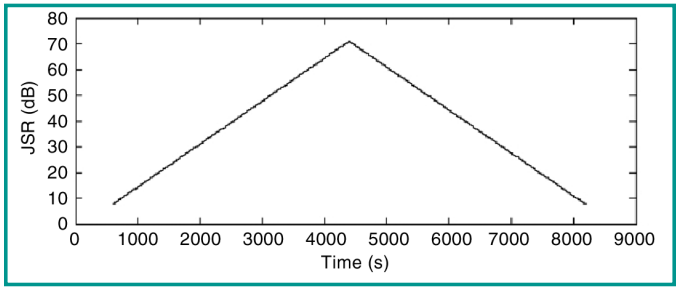

FIGURE 1 Jamming-to-signal ratio (JSR) during the simulations

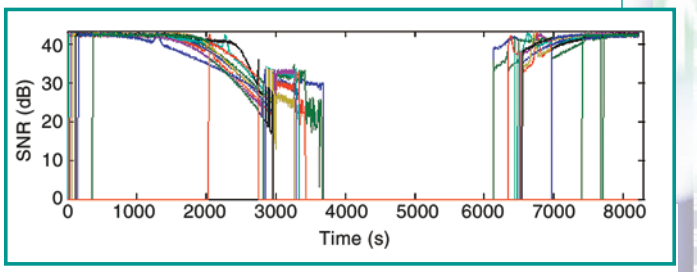

FIGURE 2 SNR of all channels in tracking mode. (0 dB means no tracking.)

to feed several commercially developed GPS receivers.

We used three receiver types of different makes and different levels of sophistication for the investigations: a receiver introduced in 1994 using arrow-correlator technology but no longer on the market, an OEM sensor currently on the market, and a recently introduced receiver for machine control.

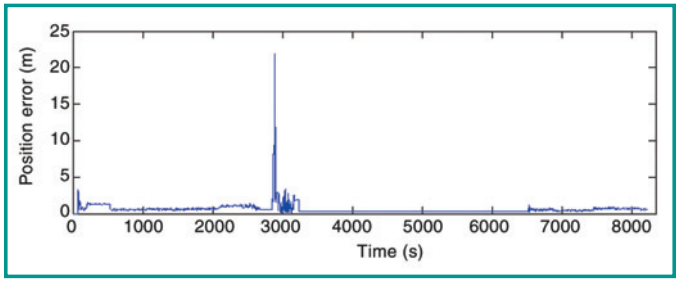

FIGURE 3 Position accuracy during a simulation interval with jamming (the smooth part between 3300 and 6500 seconds means no tracking). CCW jamming of narrow-correlator receiver.

Scenarios

We designed seven different jamming scenarios including one without jamming. In order to isolate the effects of the jamming signal types, as many variables as possible were kept identical in the different scenarios. These "static" variables include, among others, receiver position, GPS signal level, UTC of the scenario runtime, and the ionospheric and tropospheric models. (These models were in accordance with NATO Standardization Agreement (STANAG) 4294, Issue 1.) Modeling of multipath effects is possible with the simulator system, but was not utilized during the simulations. Only the jamming signal types were changed from scenario to scenario.

The different jamming signals used were:

- Non-Coherent Continuous Wave (NCW)
  Frequency: 1575.42 MHz
- Coherent CW (CCW)
  Frequency: 1575.42 MHz
- Swept CW (SCW)
  Center frequency: 1575.42 MHz
  Sweep waveform: Triangle
  Repetition rate: 1 kHz
  Frequency deviation: ±50 kHz
- Amplitude Modulation (AM)
  Carrier frequency: 1575.42 MHz
  Modulation waveform: Sine
  Modulation frequency: 1 kHz
  Modulation depth: 50.0 percent
- Frequency Modulation (FM)
  Carrier frequency: 1575.42 MHz
  Modulation waveform: Sine
  Modulation frequency: 1 kHz
  Frequency deviation: ±50 kHz
- Band-limited White Noise
  Center frequency: 1575.42 MHz
  Bandwidth: 20 MHz

(See "Signal Modulation — The Basics" sidebar on page 54 for a description of modulation types.)

Parameters. The jamming signal level was varied from −122 decibels referenced to 1 milliwatt (dBm) to −59 dBm and back to −122 dBm in 0.5 dB steps in all the jamming scenarios (see **Figure 1**). The seventh scenario in which no jamming signal was introduced provided a reference for the various jamming scenarios.

In all scenarios, the following parameter values were used:

Latitude N 63° 25′ 6.7745″, longitude E 10° 23′ 57.2180″, height 106 meters;

Power received at L1 from each GPS satellite: −130 dBm;

Length of each session: 2 hours, 20 minutes (see, also, Figure 1);

8 dB < JSR < 71 dB (that is, −122 dBm < J < −59 dBm), where J is the jamming signal power and JSR is the jamming signal to GPS signal power ratio.

Simulations

The number of satellites tracked was one indicator used for assessing receiver vulnerability to jamming, as this parameter is important with regard to position accuracy. In general, the more satellites in view, the better the possibilities for good position accuracy. This is due to the fact that a receiver having many satellites accessible can avoid tracking an excessive number of low-elevation-angle satellites with low signal-to-noise ratio (SNR). (Some low-elevation-satellites must always be tracked for geometrical reasons.)

In tracking mode, it is particularly interesting to observe receiver transitions from four to three satellites (from 3D to 2D navigation, with the receiver height held constant) and transitions from one to zero satellites (that is, from some tracking to no tracking).

When a receiver is in search mode, it is correspondingly interesting to observe transitions in the opposite direction, that is, when the receiver is regaining navigation capability.

The SNR deteriorates in the presence of interfering signals. There is a variation in SNR during a jamming test because of the varying instantaneous interference level, leading to corresponding variations of position accuracy. As an example, **Figure 2** shows the SNR values of all tracked channels during a simulation interval (CCW jamming of the narrow-correlator receiver). SNR values are those provided by the receiver log file. The SNR values in this figure and elsewhere in the article are actually the SNR in a 1 Hz noise bandwidth.

When a "good" satellite (one with favorable geometry and a healthy SNR) is lost, there is a sharp decline in position accuracy which continues until a replacement satellite has been acquired or the lost satellite has been reacquired (see **Figure 3**).

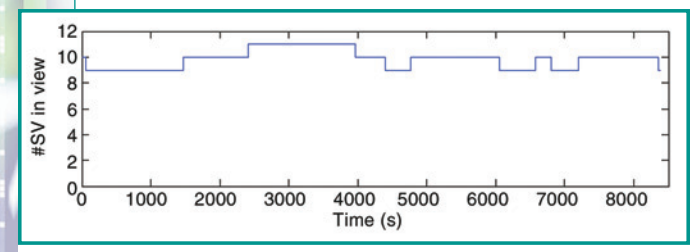

FIGURE 4a OEM receiver: Number of satellites in view

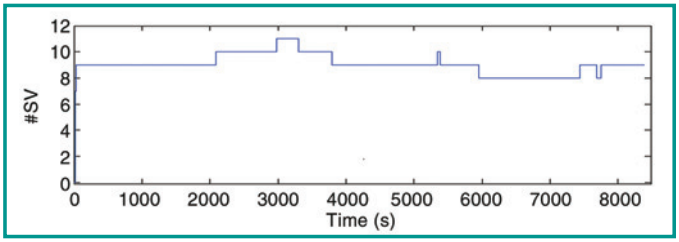

FIGURE 4b Number of satellites used for the position determination

Test Results

As we mentioned above, the reference scenario contains no jamming/interfering signals. Figure 4 illustrates such normal performance for the OEM receiver. It is seen that tracking for 3D navigation is achieved a few seconds after start. The corresponding position errors are shown in Figure 4c.

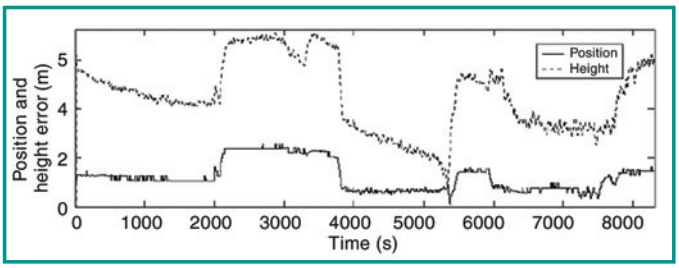

FIGURE 4c Position errors corresponding to Figure 4b (horizontal error: solid line, vertical error: stippled line)

Referring to the discussion of scenarios above, the effects of AM, FM, and noise jamming on the same (that is, OEM) receiver are used as examples. Numerical values are given in Tables 1–3.

For the sake of comparison, corresponding diagrams and tables are shown below for the machine-control receiver (Figures 5 a–c and Tables 2 a–c).

Except for differences in specific threshold values, the OEM and machine-control receivers largely show similar behavior. SNR values decline with increasing interfering signal level and rise with decreasing inter-

Signal Modulation — The Basics

A radio wave, or any electromagnetic wave for that matter, may be generally characterized by four parameters: amplitude, frequency, phase, and polarization (the direction of its electric field vector). If the values of amplitude, frequency and polarization remain constant, then the wave is a pure oscillation or "tone" and can be represented as a sine wave. (The phase of a sine wave at a fixed position in space varies as $2\pi f t$ where f is the frequency and t is time.)

An unvarying tone doesn't convey any information. However, the wave can be modulated by varying one or more of its characteristic parameters in a controlled fashion. In this way information, whether it be audio, images, or data, can be transmitted from one place to another. The sine wave is therefore referred to as a "carrier" (of the modulation). A continuous wave, or CW for short, is a wave that is not interrupted.

Of course, radio waves are not only used for communicating. They're also used for navigation, radar, and many other purposes including the jamming of other radio signals. The modulating signal may either be continuously varying (analog) or have a fixed number of values of one or more of the parameters (digital) — two values in the case of binary modulation.

CW signals of different forms can be used for jamming. If the CW jamming signal has the same frequency as the "target" signal but is not in phase with it, the jamming is non-coherent. If the jamming signal is in phase with the target, the jamming is coherent. It is also possible to sweep the CW jamming signal over a range of frequencies centered on the target signal's frequency: swept CW (SCW). For example, every millisecond the jammer frequency could be swept linearly from 50 kHz below the target frequency to 50 kHz above it and back again.

Amplitude modulation (AM) is commonly used for broadcasting and communications. For example, long wave (30-300 kHz), medium wave (300 kHz – 3 MHz), and short wave (3-30 MHz) radio broadcasting uses AM as do some aeronautical communications. If a continuous wave is interrupted by keying the transmitter on and off using a code of some kind, such as Morse code, information can be sent. Consequently, Morse code radio transmissions are often referred to as CW communications, although other modulation techniques are now used for radiotelegraphy.

On-off keying can also be used to transmit commands to equipment or for low-data-rate messaging. For speech and music transmission, an audio waveform is modulated onto the carrier. The highest audio frequency which can be conveyed depends on the allocated bandwidth of the signal. The total bandwidth of an AM signal is twice the highest modulation frequency. Typically, AM broadcasting is low fidelity with bandwidths of about 10 kHz or so. The modulation depth (the ratio of the peak change in carrier amplitude to the unmodulated carrier amplitude, expressed as a percentage) must not exceed 100 percent. An AM jamming signal can be modulated with a pure audio tone, say of 1 kHz with a modulation depth of 50 percent.

Frequency modulation (FM) is used for very high frequency (VHF, 30-300 MHz) high fidelity broadcasts and for communications in the VHF and ultra-high frequency (UHF, 300 MHz – 3 GHz) ranges of the radio spectrum. The instantaneous carrier frequency changes with the frequency and amplitude of the modulating waveform. The transmitted bandwidth is governed by the ratio between the frequency deviation (how much the instantaneous frequency departs from the assigned carrier frequency) and the modulating frequency. An FM jamming signal might use a pure sinusoidal modulating waveform with a frequency of 1 kHz and with a frequency deviation of ± 50 kHz.

Phase modulation (PM) is typically used for data transmissions and, as we know, it modulates the GPS signal carriers with the pseudorandom noise codes and the navigation message. For jamming purposes, the phase of the carrier can be randomly varied to create a white-noise jammer. (White noise has a Gaussian voltage distribution with a zero mean and a uniform phase distribution between 0 and 2π.) The rapidity with which the phase changes are made will determine the bandwidth of the jammer. If the bandwidth were 20 MHz, for example, the jamming signal would essentially overlay the whole GPS signal.

While the polarization of a wave can be modulated to transmit information, this is not very common. – *R.B.L.*

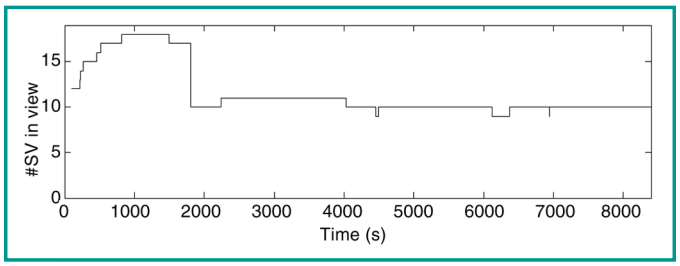

FIGURE 5a Machine-control receiver: number of satellites in view (Erroneous receiver indication of more than 11 satellites in view)

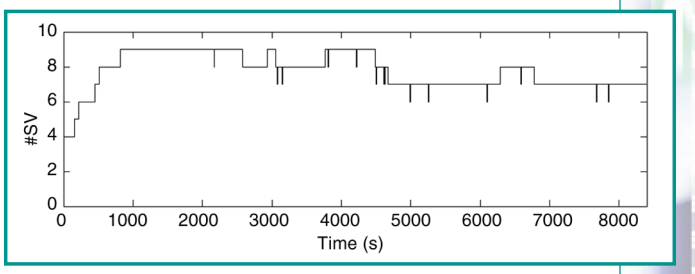

FIGURE 5b Number of satellites used

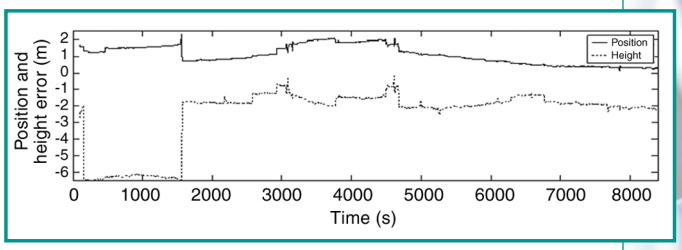

FIGURE 5c Position errors (horizontal error: solid line, vertical error: stippled line)

ference. Position errors are maximum just before the loss of lock and just after regaining lock.

However, there is sometimes a considerable difference in error magnitudes between the receivers during such a transition, as the OEM receiver's errors can be many kilometers in spite of the receiver indicating a valid position, whereas the machine-control receiver errors are only a few meters. A peculiar similarity (see **Table 3**, next page) is that both receivers fail to regain navigation capability within the interval after having been jammed by a swept continuous wave. This is in contrast to the narrow-correlator GPS receiver. (4/3 means loss or regaining of 3D navigation, 1/0 means loss/acquisition of the last/first satellite.)

The narrow-correlator receiver has a special feature which disables position updates if more than four channels have SNR values less than 30 dB. The "last valid position" and "first valid position" columns in Table 3 show at what JSR level four or more channels had SNR values of 30 dB or higher after losing/regaining lock.

Discussion and Conclusions

The narrow-correlator receiver does not deliver position data if fewer than four satellites have signal-to-noise ratios exceeding 30 dB. Thus, the last valid position really defines the upper JSR limit for navigation with this receiver and not the loss-of-lock value which is used for the other two receivers.

The narrow-correlator receiver has an anti-jam mode which, however, did not detect the AM signal. This is assumed to explain why it was most vulnerable to the AM signal (see Table 3), in contrast to the other receivers, where AM is listed in fifth place with regard to efficiency of jamming.

The transitions between tracking of three and four satellites and between one or no satellite show that the FM signal is most efficient (that is, requires the smallest JSR) for the narrow-correlator and OEM receivers. For the machine-control receiver, the SCW signal is the most efficient one, although the FM signal is only 0.5 dB worse. All in all, we therefore conclude that all three receivers as a group are most vulnerable to the FM jamming signals. However, we also conclude that the JSR values causing loss of navigation capability are quite different for the three receivers as shown by Table 3.

Plain noise turned out to be the least efficient type of jamming signal as it requires the highest JSR to cause loss of navigation capability for all three receivers. Noise jamming requires 13–15 dB higher JSR values for loss of lock than FM jamming of the narrow-correlator and OEM receivers, whereas the dif-

TABLE 1a Results of AM jamming of the OEM receiver

Parameter	JSR (dB)	SNR (dB)
Beginning to lose track	36.5	34.5 (ensemble)
Loss of 3D navigation	39.0	31.8 (ensemble)
Complete loss of navigation	40.5	33.5 (ensemble)
Regaining 2D navigation	13.5	49.0 (ensemble)
Regaining 3D navigation	13.5	49.0 (ensemble)

TABLE 1b Results of FM jamming of the OEM receiver

Parameter	JSR (dB)	SNR (dB)
Beginning to lose track	35.5	35.0 (ensemble)
Loss of 3D navigation	36.0	34.5 (ensemble)
Complete loss of navigation	36.0	34.5 (ensemble)
Regaining 2D navigation	17.5	48.7 (ensemble)
Regaining 3D navigation	16.0	49.0 (ensemble)

TABLE 1c Results of noise jamming of the OEM receiver

Parameter	JSR (dB)	SNR (dB)
Beginning to lose track	53.0	31.0 (ensemble)
Loss of 3D navigation	53.0	30.0 (ensemble)
Complete loss of navigation	53.5	30.1 (ensemble)
Regaining 2D navigation	48.0	36.7 (ensemble)
Regaining 3D navigation	47.5	36.1 (ensemble)

TABLE 2a Results of AM jamming of the machine-control receiver

Parameter	JSR (dB)	SNR (dB)
Beginning to lose track	40.0	35.5 (ensemble)
Loss of 3D navigation	45.5	32.7 (ensemble)
Complete loss of navigation	45.5	33.0 (ensemble)
Regaining 2D navigation	38.0	38.3 (ensemble)
Regaining 3D navigation	37.5	39.3 (ensemble)

TABLE 2b Results of FM jamming of the machine-control receiver

Parameter	JSR (dB)	SNR (dB)
Beginning to lose track	31.0	40.5 (ensemble)
Loss of 3D navigation	40.5	33.7 (ensemble)
Complete loss of navigation	41.0	33.7 (ensemble)
Regaining 2D navigation	34.5	35.0 (ensemble)
Regaining 3D navigation	32.5	37.2 (ensemble)

TABLE 2c Results of noise jamming of the machine-control receiver

Parameter	JSR (dB)	SNR (dB)
Beginning to lose track	40.5	38.8 (ensemble)
Loss of 3D navigation	48.5	32.0 (ensemble)
Complete loss of navigation	48.5	32.0 (ensemble)
Regaining 2D navigation	43.5	36.3 (ensemble)
Regaining 3D navigation	43.0	36.4 (ensemble)

TABLE 3 Summary of results. Tests 1, 8 , 15 were non-jamming reference tests.

Test no.	Receiver	Type of interference	Last valid position	JSR (dB) at loss of lock: 4/3 SV	JSR (dB) at loss of lock: 1/0 SV	JSR (dB) when regaining lock: 4/3 SV	JSR (dB) when regaining lock: 1/0 SV	First valid position
2	Narrow-correlator	CCW	51.5	53.5	59.0	36.0	42.0	35.5
3	N-c	FM	47.0	48.0	49.0	26.0	40.5	26.0
4	N-c	NCW	53.0	57.5	60.0	37.0	42.5	37.0
5	N-c	Noise	53.5	58.0	58.0	46.5	47.0	46.0
6	N-c	SCW	50.0	52.5	52.5	33.5	42.0	25.0
7	N-c	AM	43.0	50.5	65.5	31.0	35.5	31.0
9	OEM	CCW	_	38.5	38.5	18.5	18.5	_
10	OEM	FM	_	36.0	36.0	16.0	17.5	_
11	OEM	NCW	_	38.0	38.0	27.5	27.5	_
12	OEM	Noise	_	53.0	53.5	47.5	48.0	_
13	OEM	SCW	_	38.0	39.0	_	_	_
14	OEM	AM	_	39.0	40.5	13.5	13.5	_
16	Machine-control	CCW	_	44.0	44.0	31.0	32.0	_
17	M-c	FM	_	40.5	41.0	32.5	34.5	_
18	M-c	NCW	_	44.5	45.0	32.5	33.0	_
19	M-c	Noise	_	48.5	48.5	43.0	43.5	_
20	M-c	SCW	_	40.0	40.0	_	_	_
21	M-c	AM	_	45.5	45.5	37.5	38.0	_

ference in the machine-control receiver case is about 8 dB.

The narrow-correlator receiver differs in its response from the other two receivers with regard to its 1/0 transition in the case of AM jamming, where the limit is as high as 65.5 dB. This is seemingly in contradiction to its behavior at the 4/3 threshold where AM is the most efficient jamming signal. However, we suspect that the receiver just locked onto the jamming signal (rather than the GPS signal) in the former case. This assumption is strengthened by the fact that the Doppler shift of the GPS signal at the time was almost constant at 3 kHz. This phenomenon has also been investigated by others, and it has been shown that a GPS receiver's tracking loops sometimes can lock onto jamming signals.

Turning to a receiver's ability to regain navigation capability following cessation of jamming, we note that the values of Table 3 clearly show that noise is the least efficient type of jamming signal. The most efficient type turned out to be the swept continuous wave which, in fact, prevented the OEM and machine-control receivers from locking onto GPS signals at all values of JSR used for the simulations.

As a general conclusion, it is clear that a modulated interfering signal is far more dangerous to a GPS receiver than noise of the same power level. The worst type of modulation varies, depending on receiver construction. For the receivers we examined, however, the FM signal was most efficient in the receiver tracking mode and the swept continuous wave in the search mode.

Further Reading

For an introduction to navigation warfare, see:

"And the Compass Spun Round and Round. The Coming Era of Navigation Warfare," by D. Herskovitz in *Journal of Electronic Defense*, Vol 20. No. 5, May 1997, pp. 35-39; 65.

For earlier studies of the effects of interference on civil GPS receivers, see:

Analysis of Radio Frequency Interference Effects on a Modern Coarse Acquisition (C/A) Code Global Positioning System (GPS) Receiver, by K.D. Johnston, M.S. thesis, The Air Force Institute of Technology, 1999. An on-line version is available at: <https://research.au.af.mil /papers/ ay1999/afit/gso-eng-99m-02.pdf>.

"A Growing Concern: Radiofrequency Interference and GPS" by F. Butsch in *GPS World*, Vol. 13, No. 10, October 2002, pp. 40-50.

For an account of accidental jamming of GPS receivers, see:

"Rogue Transmitter Knocks out GPS Signals" by B. Brewin in *Federal Computer Week*, April 13, 1998, p. 1. An on-line version is available at <http://www.fcw.com/ fcw/ articles/1998/FCW_041398_310.asp>.

For a detailed overview of the vulnerability of GPS, see:

Vulnerability Assessment of the Transportation Infrastructure Relying on the Global Positioning System – Final Report. John A. Volpe National Transportation Systems Center, Cambridge, Massachusetts, August 29, 2001. An on-line version is available at: <http://www.navcen.uscg.gov/news/archive/2001/Oct/FinalReport-v4.6.pdf>.

Acknowledgements

This article is based on a paper presented at NAV 02, GNSS Vulnerability, hosted by the Royal Institute of Navigation, November 5-7, 2002, in London, United Kingdom.

Manufacturers

The narrow-correlator receiver used in these tests was a **NovAtel Inc.** (Calgary, Alberta, Canada) *GPSCard 951R;* it is no longer on the market. The OEM sensor was a **Garmin Ltd.** (Olathe, Kansas) *GPS 25*. The machine-control receiver was a **Leica Geosystems AG** (Heerbrugg, Switzerland) *MC500 GPS* sensor.

The interference generator was an *STR 2765* and the GPS signal simulator an *STR 4760*, both from Global Simulation Systems, now a unit of **Spirent Communications** (Paignton, Devon, United Kingdom).

"Innovation" is a regular column featuring discussions about recent advances in GPS technology and its applications, and the fundamentals of GPS positioning. The column is coordinated by Richard Langley of the Department of Geodesy and Geomatics Engineering at the University of New Brunswick, who appreciates receiving your comments as well as topic suggestions for future columns. To contact him, see the "Columnists" section on page 2 of this issue.