



COMPANY CONFIDENTIAL

NLR-CR-2008-671

Electromagnetic Interference on Low Cost GPS Receivers

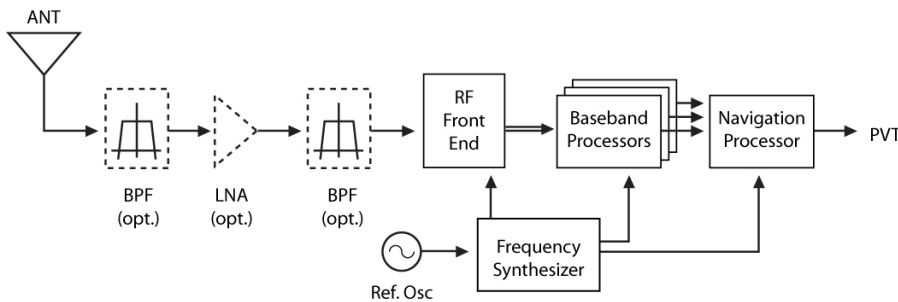
S. Storm van Leeuwen





Executive summary

Electromagnetic Interference on Low Cost GPS Receivers



Problem area

For the position determination of vehicles, a low cost GPS receiver is an important component in the On Board Unit, anticipated to be used in the project ‘Anders Betalen voor Mobiliteit’ (ABvM).

GPS receivers are vulnerable to unintentional radiation from nearby radio transmitters, and to intentional radiation such as jamming, meaconing and spoofing.

The National Aerospace Laboratory NLR of The Netherlands has been contracted to investigate the vulnerability of low cost GPS receivers to (un)intentional radiation and to identify means to detect and mitigate effects of (un)intentional radiation.

Description of work

The architecture typical for low cost GPS receivers is described. The vulnerability of the circuit blocks in

the receiver to radiation and the means to detect the presence of radiation are identified. Emphasis is placed on the effects of jamming, meaconing and spoofing. Means to mitigate the effects of radiation are identified.

This report is based only on publications in the open domain.

Conclusions and recommendations

Vulnerability

The vulnerability of low cost GPS receivers to (un)intentional radiation has been shown in several publications. Broadband noise and continuous wave interference signals within the pass band of the GPS Coarse Acquisition (C/A) code signal pose the larger jamming threats. Interference signals with a power factor of 30 (15dB) above the GPS signal level already degrade the receiver performance.

Report no.

NLR-CR-2008-671

Author(s)

S. Storm van Leeuwen

Report classification

COMPANY CONFIDENTIAL

Date

October 2008

Knowledge area(s)

Third Party Risk & Policy Support

Descriptor(s)

GPS
interference
jamming
spoofing
meaconing

Detection

The presence of jamming interference can be detected by already available signals within the receiver such as automatic gain control, signal and noise power, and carrier to noise ratio (C/N_0).

Meaconing and spoofing can be detected by non-coherences between the so-called 'raw data' (pseudoranges, carrier phases, Doppler shifts, and the navigation data as modulated by 50 bits per second on the satellite signal). They can also be detected by non-coherences with navigation data collected earlier, or received via an alternative path such as GSM. Integration with other sensors such as inertial sensors can increase the detection success of jamming, meaconing and spoofing.

It is recommended to use these detection signals to flag a malfunction to the vehicle driver.

Mitigation

The circuit blocks in the receiver can be designed in such a way that the harmful effects of radiation are reduced. A number of measures are recommended:

- Optimized antenna design,
- High energy pulse protection for the first amplifier directly downstream of the antenna,
- An analogue to digital signal converter with at least 1,5 bit resolution, 2 bits is preferred,
- A wide automatic gain control range (~50dB) to allow resistance

against reasonable levels of (un)intentional radiation,

- A high sensitivity baseband processor,
- Other advanced techniques such as pseudorange (de)weighting and receiver autonomous integrity monitoring (RAIM),
- integration with other sensors such as inertial sensors to increase the robustness against jamming.

The above recommended measures concern hardware, firmware and software of the receiver. It is believed that implementation of these measures by the receiver manufacturer is feasible within the cost constraint of the ABvM project.

Follow-up work

Finally it is recommended to investigate in the laboratory a number of commercially available low cost GPS receivers, which may be candidates for the ABvM On Board Unit.

This investigation will establish the actual vulnerability of these receivers for (un)intentional radiation, and will prove the value of the proposed means to detect radiation and to mitigate the effects.

Applicability

This report can be used as an input to the procurement specification for the On Board Units.



COMPANY CONFIDENTIAL

NLR-CR-2008-671

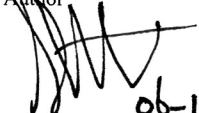

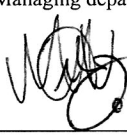
Electromagnetic Interference on Low Cost GPS Receivers

S. Storm van Leeuwen

No part of this report may be reproduced and/or disclosed, in any form or by any means without the prior written permission of the owner.

Customer Min V&W
Contract number 4500128156
Owner Min van V&W
Division NLR Aerospace Systems & Applications
Distribution Limited
Classification of title Unclassified
 October 2008

Approved by:

Author	Reviewer	Managing department
 06-11-2008	 7/11/2008	 07-11-2008

COMPANY CONFIDENTIAL



Contents

1	Introduction	7
2	Expected types of interference	8
2.1	Jamming	8
2.1.1	Broad band noise	8
2.1.2	Narrow band, carrier	9
2.1.3	Narrow band, Amplitude Modulation (AM)	9
2.1.4	Narrow band, Frequency Modulation (FM)	9
2.1.5	Narrow band, noise	9
2.1.6	Pulse	9
2.2	Meaconing	10
2.3	Spoofing	10
3	Architecture of low cost GPS receivers	11
3.1	(Active) antenna	11
3.2	Front end	13
3.3	Base band processor	14
3.3.1	Code acquisition	14
3.3.2	Code-carrier tracking	16
3.4	Navigation processor	20
3.4.1	Conversion to raw data	20
3.4.2	Position, velocity and time calculation	20
3.5	High sensitivity GPS	21
4	EMI effects, detection and mitigation	23
4.1	Antenna	23
4.2	Front end	23
4.3	Baseband processor	25
4.3.1	Code acquisition	25
4.3.2	Code- carrier tracking	27
4.4	Navigation processor	29
4.4.1	The role of C/N_0 revisited	29
4.4.2	Code minus carrier combination	30
4.4.3	Data coherence	30



4.4.4	Receiver Autonomous Integrity Monitoring	32
4.4.5	Spoofing and Meaconing	32
4.5	Integration with other sensors	32
5	Low cost receiver output for EMI detection	33
6	Conclusion and recommendations	35
6.1	Conclusions	35
6.1.1	Antenna	35
6.1.2	Front end	35
6.1.3	Base band processor, acquisition state	36
6.1.4	Base band processor, tracking state	36
6.1.5	PVT calculation	36
6.2	Recommendations	37
6.2.1	Recommendations with respect to EMI detection	37
6.2.2	Recommendations with respect to EMI mitigation	38
	Referred publications	39
	Other relevant publications	40
Appendix A	Uncorrelated signals	41



Abbreviations

ABvM	Anders Betalen voor Mobiliteit
ADC	Analogue to Digital Converter
AGC	Automatic Gain control
AGPS	Assisted GPS
AM	Amplitude Modulation
AWGN	Additive White Gaussian Noise
BB	Base Band
BPF	Band Pass Filter
Bps	bits per second
BW	Band Width
C/A	Coarse Acquisition
C/N ₀	Carrier to Noise ratio
COP	Correlator Output Power
CW	Continuous Wave
E	Early
EMI	ElectroMagnetic Interference
FE	Front End
FM	Frequency Modulation
GPS	Global Positioning System
I	In phase (signal)
I&D	Integrate and Dump
IF	Intermediate Frequency
J/S	Jamming to Signal ratio
L	Late
LHCP	Left Hand Circular Polarized
LNA	Low Noise Amplifier
LPF	Low Pass Filter
N ₀	Noise measured in a one second interval
NCO	Numerically Controlled Oscillator
OBU	On Board Unit
P	Prompt
PIN diode	Positive Intrinsic Negative diode
PRN	Pseudo Random Noise
PVT	Position, Velocity and Time (solution)
Q	Quadrature (signal)



RAIM	Receiver Autonomous Integrity Monitoring
RF	Radio Frequency
RHCP	Right Hand Circular Polarized
RSS	Root-Sum-Square
T_{int}	Integration time
VGA	Variable Gain Amplifier



1 Introduction

Position determination using the Global Positioning System (GPS) is an important component in the project 'Anders Betalen voor Mobiliteit' (ABvM). The On Board Unit (OBU) contains amongst others a low-cost GPS receiver with properties as found in car navigation and recreational receivers.

The low signal level at the receiver makes any GPS receiver inherent vulnerable to ElectroMagnetic Interference (EMI) [1]. This is not only the case for low cost receivers but also for receivers for professional applications as aircraft and ship navigation and geodetic measurements. Several studies have been carried out into the EMI sensitivity of GPS receivers, with main sub-questions: how to detect, how to identify and how to mitigate the effect of EMI. In this report unintentional EMI is called '*interference*', intentional EMI is called '*jamming*'. Interference originates from sources such as radio, TV, wireless communication and radars. Interference is usually location bounded, the impact is predictable, and in general interference degrades the receiver position determination performance.

Jamming originates from transmitters with the aim to deny the correct functioning of GPS receivers. Jamming is considered to be a fraudulent operation in the context of ABvM.

Not only jamming but also *meaconing* and *spoofing* [1] are intentional EMI signals to degrade the proper functioning of GPS receivers. Jammers, meaconers and spoofers may be located inside the vehicle, or may be at an external (fixed) location elsewhere.

This report discusses the expected effects of EMI, meaconing, and spoofing on low cost receivers to be used in the OBU. Because of the higher implementation complexity meaconing and spoofing are expected to be less frequently applied than jamming. The effect of interference on the receiver is usually limited, whilst jamming can stop the receiver from functioning. For these reasons the emphasis in this report is on jamming.

In chapter 2 an overview is given of the types of EMI. In chapter 3 an inventory is made of the architecture of low cost receivers as far as applicable to EMI. Based on theoretical and measured values found in the open literature the effect of EMI on typical receiver architectures is estimated in chapter 4. In chapter 5 the required and available output quantities of low cost receivers to detect and EMI are given. Finally conclusions and recommendations are given. There are several ways to mitigate the effect of EMI, meaconing and spoofing. Probably the most effective one is to locate and eliminate the source. Mitigation however is not the prime goal of this investigation and is only touched upon wherever practical.



This study is based only on information available from public resources, and assumes that the reader is familiar with the GPS system characteristics and the limitations of low-cost GPS receivers.

2 Expected types of interference

EMI can be divided into three categories: Jamming, Meaconing and Spoofing:

- Jamming is simple; it takes little money to realize. A search on the Internet with ‘GPS jamming’ provided approx. 22000 hits (5 August 2008) with several commercially available systems in the first ten hits. In section 2.1 several forms of jamming are identified.
- Meaconing is a more sophisticated technique and consists of the re-transmission of a earlier received of GPS signal. This technique has 904 hits, and is briefly discussed in section 2.2.
- Spoofing is the most sophisticated form of EMI and consists of the transmission of artificial GPS signals with false information (‘GPS spoof’ provided 78 hits). Spoofing is briefly treated in section 2.3.

2.1 Jamming

In the context of this investigation jamming is the intentional transmission of electromagnetic radiation in a band around the GPS L1 carrier frequency (1575.42MHz for low cost receivers). The bandwidth of low cost receivers is usually limited to 2MHz around the carrier frequency. Jamming occurs in three main forms: broad band noise, narrow band signal and pulsed signals. In the subsections below the properties of the various types of jamming are given, their possible effect on GPS receivers is estimated.

The techniques required to build a jammer are simple and required electronics are readily available. Therefore the ‘threat level’ for this technique is high.

2.1.1 Broad band noise

Broad Band noise (also called Additive White Gaussian Noise, AWGN) is a noise signal with a constant power level within the GPS Coarse Acquisition (C/A) code band of approx. 2MHz width. Its level is expressed in power per frequency unit, usually dBm/Hz.

Thermal noise is broad band, and at an ambient temperature of approx. 15 degrees C has a value of -174dBm/Hz. Within a band of 2MHz (63dB-Hz) its power is -111dBm. Thermal noise can be considered as a form of interference.

The GPS signal with a power of -130dBm [1] is well below the thermal noise power. The challenge of the GPS receiver is therefore to retrieve the signals buried in thermal noise through a correlation process. Any intentional or unintentional increase of the noise level raises this



challenge, until the required original signals can no longer be retrieved (i.e. receiver stops functioning).

2.1.2 Narrow band, carrier

Narrow band carrier (pure tone or Continuous Wave, CW) is identified by its carrier frequency and power. The frequency can be constant or it can vary ('swept carrier'). Because of the periodicity of the C/A code of 1 msec the GPS signal spectrum has a large number of peaks spaced at 1kHz intervals around the GPS carrier frequency. When the jammer frequency coincides with a peak in the GPS spectrum, degradation, loss of lock, or the inability of (re-) acquisition will occur at already a relatively low jamming power. Usually only one satellite at a time is affected.

Due to the speed of a GPS satellite relative to the receiver (for an automobile roughly between -1 and +1km/sec), the GPS carrier frequency experiences a Doppler shift between -5kHz and +5kHz. With a fixed jammer frequency the spectral peaks will coincide only temporarily with the jammer frequency. At a rapidly varying jammer frequency (swept CW) degradation will occur more often.

2.1.3 Narrow band, Amplitude Modulation (AM)

An amplitude modulated carrier with the same maximum amplitude as a CW signal will degrade the receiver less compared to CW [2]. For this reason the presence of AM modulated signals will mostly be unintentional. It can result from higher harmonics or intermodulation products of broadcasting transmitters, amateur transmitters and mobile communication systems.

2.1.4 Narrow band, Frequency Modulation (FM)

For narrow band frequency modulated signals the remarks in 2.1.3 apply [2].

2.1.5 Narrow band, noise

A narrow band noise signal with the same power as a broad band noise signal degrades the operation of the receiver less [2]. Otherwise the effects are the same.

2.1.6 Pulse

Pulse signals can be high powered and occupy a broad frequency band. Possible sources are radar, Ultra Wide Band transmitters, transponders and engine ignition systems.

The power of a pulse signal can be high enough to saturate the input stage of a GPS receiver. After the disappearance of the pulse it can take some time before the input stage recovers from saturation. Depending on the duty cycle of the pulse signal and the recovery time of the input stage it may remain in saturation, resulting in the receiver not functioning.



Pseudolites are ground based beacons which function as GPS satellites. Their signal level is much higher than the satellite signal and with that is an excellent source of (intersystem) interference. Interference is prevented by the pseudolite transmitting its signal in brief bursts. Thus it has the character of a pulse signal. A well designed input stage will experience little degradation of such a signal.

2.2 Meaconing

Meaconing [1] is a technique where the received GPS signal is recorded for some time and later re-transmitted. The re-transmitted signal needs only to be slightly stronger than the real GPS signal to have the receiver lock on the wrong signal.

Meaconing is more difficult to implement than jamming. First a registration needs to be made of the desired scenario. This can be done by sampling, digitizing and storing the Intermediate Frequency (IF) signal of the GPS frontend (see next chapter). At a later stage the IF signal is converted to the analogue domain, up-converted to the GPS frequency and re-transmitted. For sufficient re-transmitted signal quality the sample frequently and digitizer resolution need to be high. For example using 5 Msamples/sec and a 12 bit A/D converter provides a data stream with 7.5 MByte/sec. A recording of 1 hour requires 27 GByte storage capacity. These quantities are feasible with a modern laptop PC.

It is assumed that the realization of meaconing should be feasible for the 'advanced amateur'.

2.3 Spoofing

Compared to other techniques spoofing [1] is the most complicated one. In a spoofing scenario GPS signals are artificially generated, as is done by GPS signal simulators. A scenario is conceivable where by spoofing the GPS receiver thinks it is on a parallel road, whereas the vehicle actually is on the highway. The realization of such a form of spoofing is complex, but supposedly feasible for a highly trained defrauder. The spoof signal must only be little stronger than the real GPS signal to have the receiver to capture the spoof signal.

In a simple spoofing scenario where a trajectory is generated which deviates considerably from the real trajectory, spoofing can usually be detected. In a more sophisticated scenario the spoofed position/ velocity/ time solution can to a great extent have the same properties as other independent systems. Spoofing is then difficult to detect.

To realize the advanced spoof scenario profound knowledge and sophisticated equipment is required. It is anticipated however that this technique will become available for the mass market within 5 – 10 years.

3 Architecture of low cost GPS receivers

In this chapter the architectures of low cost receivers are given. The information has been based on open literature such as text books and data sheets. Given the short duration of this investigation it was not possible to obtain intellectual property data of manufacturers.

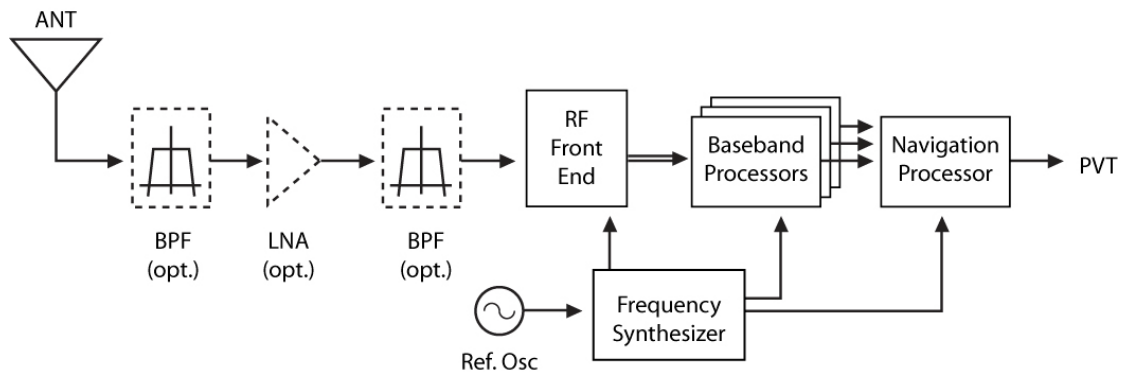


Figure 1. Receiver block diagram

The Antenna receives the GPS signal, background noise, and EMI. An optional Band Pass Filter (BPF) centered around the L1 frequency (1575.42MHz) with a Band Width (BW) of about 2MHz is used to reduce out of band noise and EMI. The filter is preferably situated in front of the Low Noise Amplifier (LNA, optional) to prevent overloading of its input by strong out of band signals.

The filtered and amplified signal is presented to the Radio Frequency (RF) Front End (FE) where it is down converted from the L1 frequency to an Intermediate Frequency (IF) between 4MHz and 100MHz, depending on the implementation of the receiver. The analogue IF signal is converted to a digital signal at a rate of about 4Msamples/sec.

The digitized IF signal is input to a number of parallel digital Base Band (BB) processors ('channels'), typically 12 to 20 for modern low cost receivers. The 'raw data' output of the baseband processors (pseudoranges, carrier phases, Doppler shifts, Carrier to Noise ratios (C/N_0), Navigation data) are presented to a general purpose processor carrying out the conversion of raw data into the Position, Velocity and Time (PVT) solution.

Frequency and timing signals are derived from a reference oscillator by a frequency synthesizer.

3.1 (Active) antenna

In the low cost segment two types of antennas are available: patch and helix. Both antennas may or may not be provided with an RF LNA (active respectively passive). Given the very small distance in the OBU between antenna and receiver, a passive antenna will probably be applied.



To reduce the impact of degradation by ‘out of band’ signals it is important that a GPS antenna resonates on the L1 the frequency, has a narrow band frequency response (approx. 2MHz), is sensitive for Right Hand Circular Polarized (RHCP) signals, and effectively suppresses non-RHCP signals.

The antenna must be sensitive in the upper hemisphere at elevation above approx. 5 degrees. Insensitivity below 5 degrees of elevation reduces the negative effect of ground-based jammers, meaconers and spoofers. This insensitivity is also needed to reduce the impact of satellite signal multipath reflections.

In the ideal case the antenna would also be insensitive in the direction of the automobile structure (figure 2) . This reduces even more the effect of in-vehicle jammers, and unintentional interference by electronic devices such as laptop, video game, etc (and multipath). A two element antenna array can be designed to have such properties. Such a (sophisticated) antenna should be adapted to the geometry of the vehicle during installation.

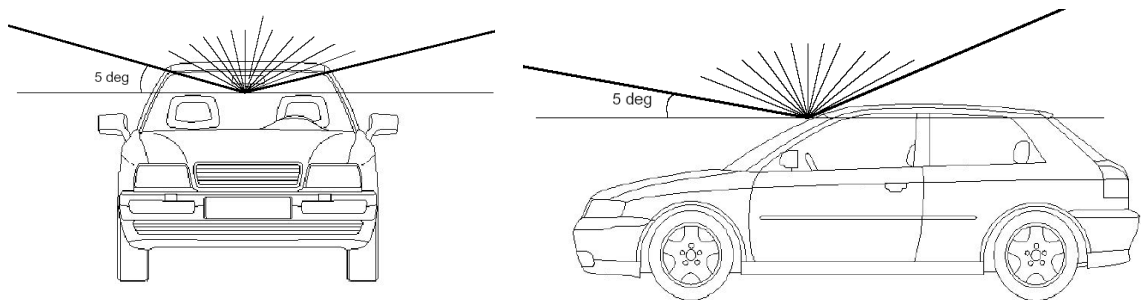


Figure 2. Radiation diagram Antenna

Both patch and helix antennas have a bandwidth in the order of 1% of the resonance frequency (approx. 15 up to 20 MHz) and exceed the bandwidth criterion. Additional narrow band filtering is required.

The filter and LNA directly after the antenna determine to a large extent the final noise contribution of receiver (electronics) to the signal. LNAs with a noise contribution of 1 dB are simply to realize, low noise narrow band filters on the other hand are much more difficult to realize. This could lead the designer to place the narrow band filter behind the LNA where its contribution to the final noise figure is less.

3.2 Front end

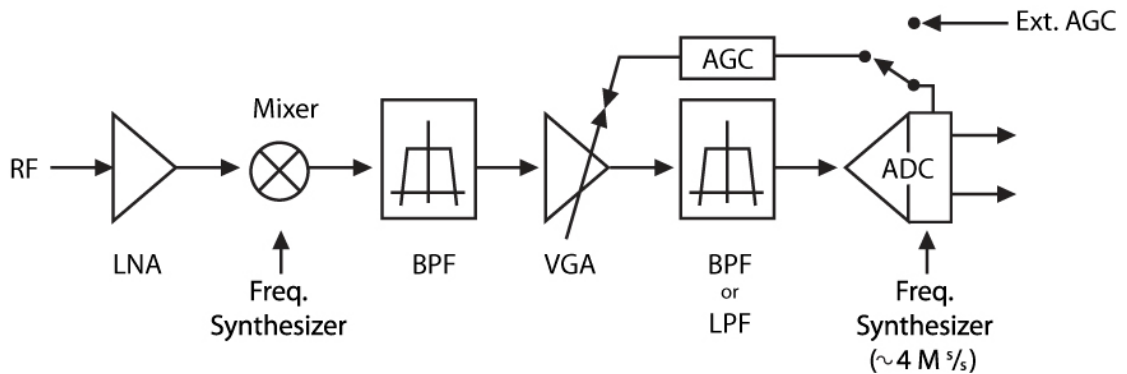


Figure 3. Front end diagram

The weak GPS signal from the antenna is filtered and amplified (LNA). The RF signal at the output of the LNA is down converted to an intermediate frequency (IF, between 4MHz and 100MHz) by mixing with local oscillator signal, filtering and amplifying. Mixing, filtering and amplifying are done in one, two or three stages depending on the manufacturers' implementation. The result is the original signal but now centered around the IF.

The GPS signal is amplified by approx. 100dB to a level of around 5V before it is presented to the Analogue to Digital Converter (ADC). The ADC number of bits can be 1 (possible digital values 1 or -1), 1.5 (1, 0, -1), 2 (3, 1, -1, -3) or 3 (7, 5, 3, 1, -1, -3, -5, -7). A minimum of 1.5 bits is required for detection of interference (and reducing the effect) [3]. The sample rate must be high enough to reconstruct the IF signal without aliasing. The sample rate depends therefore on the IF frequency and bandwidth and is normally in the order of 4 Msamples/sec. To fully exploit the input range of the ADC, Automatic Gain control (AGC) is implemented at one or more down converter amplifiers. The AGC signal can be generated inside the Front End (FE), but it can also be generated by the Base Band process. Some FEs allow a choice.

AGC is effective for converters with more than 1 bit. As will be mentioned later the AGC signal is useful for the detection (and reducing the effect) of EMI [4, 5]. A front end with a 1 bit ADC is therefore undesirable.

The digital output can be the digitized IF, or the digitized In-phase (I) a Quadrature (Q) components of the IF signal, again manufacturer dependent.

The FE functions independent of the receiver (channel) mode: acquisition or tracking. Detection of degradation by means of AGC is therefore always possible.



3.3 Base band processor

The architecture and functioning of the Base Band processor (BB) differs for a channel in acquisition mode from a channel in tracking mode. Code acquisition typically requires a 10dB higher signal to noise level compared to code tracking. Also the vulnerability to interference depends on the mode. Therefore acquisition and tracking are treated separately.

3.3.1 Code acquisition

There are two major methods for the acquisition process, the ‘time domain search’ (2-dimensional code delay-doppler freq bin) and the ‘frequency domain search’. Both are explained in the next paragraphs.

3.3.1.1 Time domain search

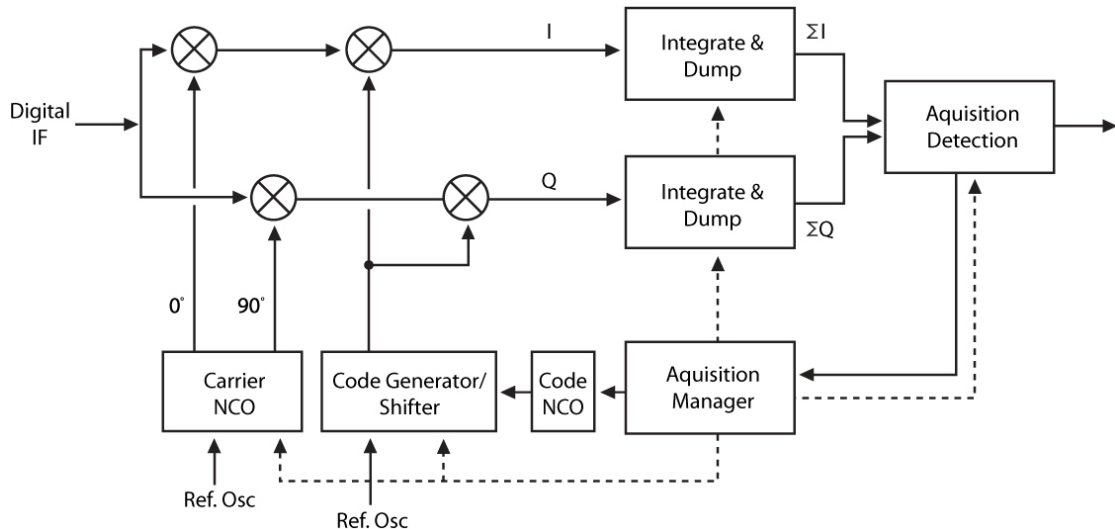


Figure 4. Simplified code acquisition diagram, one channel

A block diagram of the acquisition process is shown in figure 4 [3]. All blocks are common to the tracking process (section 3.3.2) except the acquisition manager and acquisition detector.

The received satellite signal enters the receiver with an unknown code phase and unknown Doppler shift. The task of acquisition is to detect the presence of a signal, and to obtain a first estimate of the code phase, Doppler shift, and noise threshold. As soon as this process is successful, the channel transfers to the tracking mode (see section 3.3.2).

The (1.5, 2 or 3 bits) samples from the A/D converter are mixed with (digitized samples of) a locally generated carrier frequency (carrier Numerically Controlled Oscillator, NCO) and C/A code, using the first estimate of Doppler and code phase respectively.

The Acquisition Manager controls the selected C/A code (sometimes also called Pseudo Random Number/Noise or PRN), Doppler frequency and code phase (dashed lines). During one



or more code periods (1 code period takes 1 msec) the mixed signals are integrated (Integrate and Dump Correlator, I&D). The integration time is controlled by the Acquisition Manager. The integrated (I and Q) values are processed by the Acquisition Detector. At correlation of the received signal with the locally generated signal the integrated I-value will be high, at bad or no correlation the value will be low. The integrated value is compared to a threshold value. The threshold value is determined from the I and Q values. The acquisition is considered as successful when the threshold value is exceeded. Otherwise another code phase and/or Doppler value is set by the Acquisition Manager, and the process is repeated.

Since one code period is 1023 code chips (bit periods) long, and the search has to be done at intervals of $\frac{1}{2}$ chip, there are 2046 possible values for the code phase to be examined. The possible Doppler shift for an automotive receiver is mainly determined by the speed of the satellite with regard to the vehicle: between -5kHz and +5kHz. To this interval the drift of the local oscillator must be added. The Doppler interval must be divided in steps, the size of the steps depends largely on the integration time. With an integration time of 1msec the corresponding Doppler resolution is 667Hz, hence the Doppler interval is divided into 15 steps. The number of 'cells' to examine becomes up to 30690. Each cell search takes 1 msec, the total search time for one satellite can therefore be 30.69 sec. With up to 32 satellites to search (required when no ephemeris data is available), acquisition can be a long-lasting process. Figure 5 is an example of integrated values in a limited range of code-Doppler cells.

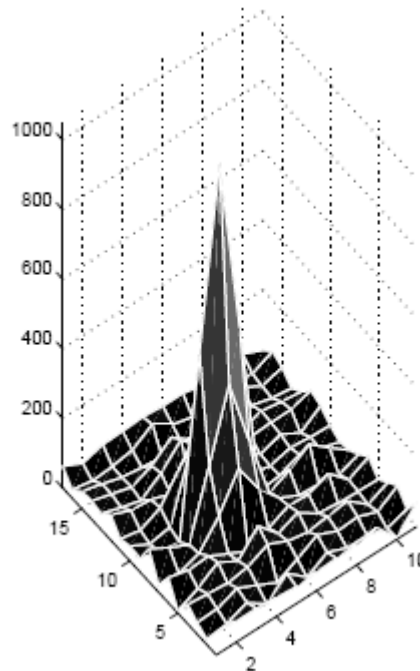


Figure 5. Part of a search space obtained with a GPS CA code with 2 samples/chip and a Doppler step of 666 Hz. (from: A Statistical Theory for GNSS Signal Acquisition)

Advance knowledge of code phase and Doppler (knowledge of estimated receiver position and time, and a recent almanac) can reduce the number of cells to be searched considerably, and can accelerate the acquisition process for one satellite to seconds.

3.3.1.2 Frequency domain search

In the ‘frequency domain search’ the Fourier transformed satellite signal is multiplied with the Fourier transform of the locally generated signal with a fixed code phase and a Doppler shift as in the time domain method. A peak in the inverse transform of the multiplied signal indicates the presence of a signal and its code phase. With this technique only the Doppler interval must be searched.

Both time and frequency domain methods perform identical in terms of acquisition success. The frequency domain search, however, requires a high amount of processing power. The time domain search lend itself well for implementation in hardware and is the most used technique in low cost receivers. Data sheets of modern BB chips sometimes mention ‘massive bank or equivalent correlators’. These receivers could be equipped with a sufficiently powerful processor to carry out the frequency search. However the data sheets give no definite answer on which method is implemented.

3.3.2 Code-carrier tracking

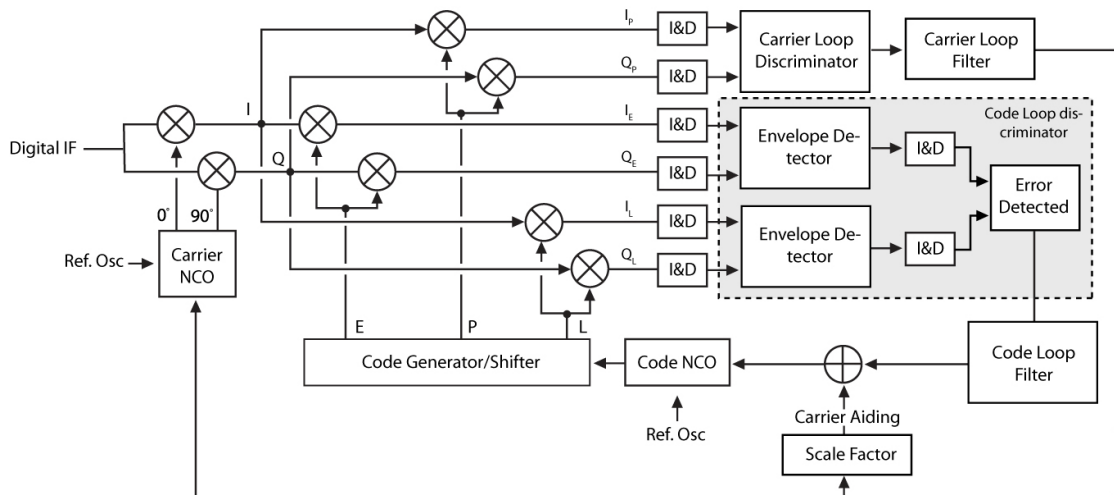


Figure 6. Code and carrier tracking – one channel

Figure 6 is simplified from figures 5.2 and 5.3 as presented in [3]. This is a typical implementation of a code/ carrier tracking channel. Many alternative architectures exist.



In the following the channel is assumed to be in steady state code- and carrier tracking mode. The transition from acquisition mode to code tracking and later to code-carrier tracking is not relevant for this investigation and will not be described further.

As in the previous subsection the digital IF signal is mixed with the replica carrier (plus carrier Doppler) generated by the carrier NCO. With the replica carrier in phase with the incoming satellite carrier the latter is removed after the mixing process (carrier wipe-off). The I-component is at maximum and contains signal plus noise, but is still buried in the noise. The Q-component contains only noise.

Next the I and Q signals are correlated (Integrate & Dump Correlator) with ‘Early’ (E), ‘Prompt’ (P) and ‘Late’ (L) local replica of the PRN code. The amount of shift between E and P, and between P and L is usually $\frac{1}{2}$ code chip. The samples are integrated (Integrate & Dump blocks, I&D) during one or more code periods. The P replica code, when in phase with the incoming satellite PRN code, produces maximum correlation between the latter and the I signal. The integrated value of the I_P branch is at maximum, the values of I_E and I_L halfway, and the Q branches at minimum. Figure 7 shows the (normalized) correlation values of E, P, and L.

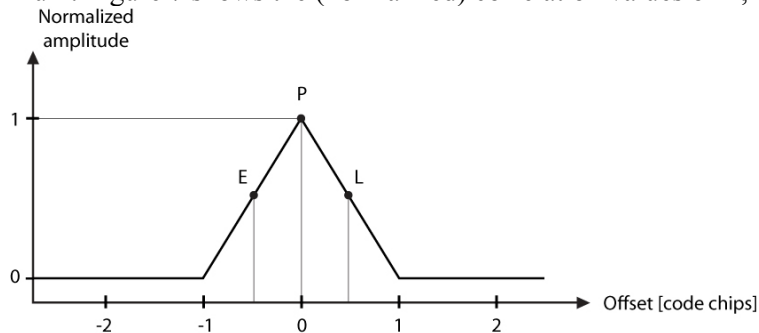


Figure 7. Normalized correlator output

3.3.2.1 Code tracking loop

The code loop discriminator uses the Early and Late values to detect any mismatch between the incoming code and the code replica. Once a mismatch between E and L is detected, an error signal is produced which adjusts the replica code phase via the code NCO to the incoming code phase.

The envelope detectors calculate the Root-Sum-Square (RSS) of I and Q, the value may be integrated again. Several algorithms exist to calculate an error signal from the RSS values. In order to estimate the error signal accurately the code loop filter reduces noise. The loop (low pass) filter order and bandwidth determine the loop filters’ response to dynamics in the incoming code.



Applying the (downscaled) error signal from the carrier loop allows reduction of the code loop bandwidth, thereby reducing code noise (decreasing pseudorange noise). Typical bandwidth is 0.1Hz to 10Hz depending on signal dynamics to be anticipated.

The replica code phase (and PRN) is the input to the navigation process.

3.3.2.2 Carrier tracking loop

The carrier loop can be implemented as a phase locked loop, a frequency locked loop or both. The discriminator operates on the I_P and Q_P values to detect phase error (phase tracking loop) or frequency error (frequency locked loop) between the incoming carrier and the replica carrier (plus Doppler). Once a mismatch is detected the (phase or frequency) error steers the carrier NCO to the incoming carrier.

The carrier loop filter reduces noise in order to estimate the error signal accurately. The (low pass) filter order, and bandwidth determine the loop filters' response to dynamics in the signal. Typical bandwidth is between 10Hz and 100Hz, depending on the signal dynamics to be anticipated.

The carrier noise expressed in length units is substantially lower than the code noise. Therefore aiding the code loop with the carrier loop error signal allows reduction of code loop bandwidth (see above). The carrier loop however requires a higher signal to noise ratio (in the order of 10dB) to remain in lock.

The replica carrier Doppler phase (or frequency) is the input to the navigation process.

3.3.2.3 Coherent and non-coherent integration

In the (coherent) integration blocks downstream of the code mixers signal and noise add up *algebraically* during the integration time of one or more code chips. As long as the signal does not change its sign (50Hz navigation bit boundary, see below) the integrated signal increases, while the integrated noise remains constant. It is thus advantageous to increase the integration time.

The PRN code signal is mixed with the 50 bits per second (bps) navigation message. Integration across a navigation bit boundary will start reducing the value of the integrated signal and is therefore not wanted. Knowledge of the moment at which the navigation bit changes sign can increase the coherent integration time up to 1/50 sec or 20 msec.



The sign of the coherently integrated signal is the sign of the navigation data bit. This sign is the input to the navigation process.

In a weak signal or high EMI environment it may be required to extend the integration time until there is sufficient discrimination between signal and noise (plus EMI). Non coherent integration downstream of the envelope detectors performs the *absolute sum* of signal and noise of a number of coherently integrated samples, and hence is less effective in increasing the signal to noise ratio.

Non coherent integration can extend the total integration time to a maximum of 600msec.

3.3.2.4 C/N₀ determination

The C/N₀ ratio of a channel in track is an important quantity for the quality of acquisition and tracking. It provides also information on the presence of interference. In figure 8 a block diagram of the determination of C/N₀ is given.

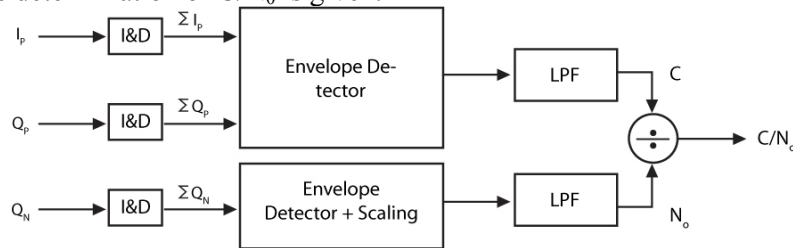


Figure 8. C/N₀ determination

With the integrated I_p, Q_p (see also figure 5) and Q_N values the C/N₀ is calculated as follows:

$$C/N_0 = C / (T_{int} * N)$$

with

$$C = \text{sqrt}(I_{PS}^2 + Q_{PS}^2),$$

$$N_0 = \text{sqrt}(I_{NS}^2 + Q_{NS}^2) \approx \text{sqrt}(2 * Q_{NS}^2) \text{ (} I_{NS} \text{ and } Q_{NS} \text{ from correlation with PRN}^1 \text{ 38)}$$

T_{int} = predetection integration time.

The above method to determine C/N₀ is called ‘correlator comparison method’. Another method is called ‘narrow to wide power ratio method’. Both methods perform well. A third method determines C/N₀ in front of the correlation process. This method is to be avoided since in the presence of interference it can under- or overestimate the true C/N₀ [3, 9].

¹ PRN 38 is not used by any satellite and hence can be used to determine the value for having no code correlation.



3.4 Navigation processor

The outputs of a single baseband processor to the navigation processor are replica code phase, replica carrier Doppler phase, sign of the navigation data bits, and integrated I and Q values. These quantities are first converted to raw data. The receiver Position Velocity and Time (PVT) solution is calculated using this raw data. The hardware used for the navigation process is usually a general purpose processor with memory and input/ output facilities. The processor is programmed using a high level language; the program is stored in non-volatile memory.

3.4.1 Conversion to raw data

The outputs of the (parallel) baseband processors are first converted to 'raw data': pseudoranges, (integrated) carrier phases, Doppler frequencies, C/N_0 numbers and the 50bps navigation data. The replica code phase is used together with the navigation data bits to determine the pseudorange for the PRN being tracked. This is a rather complicated process but of limited importance within the framework of EMI.

The replica carrier Doppler is used to estimate (integrated) carrier phase and Doppler frequency. The navigation data message is derived from the series of 50bps navigation data bits, and contains parameters such as almanac, ephemeris and satellite clock data.

3.4.2 Position, velocity and time calculation

3.4.2.1 PVT calculation

Pseudoranges of at least 4 satellites (4 baseband channels in tracking) are required to calculate 3D position and time (3 satellites for the derivation of 2D position and time). With delta carrier phases or Dopplers of at least 4 satellites the velocity can be calculated.

3.4.2.2 Receiver Autonomous Integrity Monitoring

When 5 or more satellites are being tracked, an overdetermined least squares solution produces range residuals as a by-product. When range residuals exceed a threshold value, EMI may be the cause. The challenge is to decide whether EMI, multipath, atmospheric noise, or receiver clock dynamic errors are the cause.

With $5 + N$ ($N \geq 1$) satellites being tracked and M ($1 \leq M \leq N$) satellite signals are corrupted in some way or another, an attempt can be made to identify the M satellites to exclude them from the PVT solution, thus mitigating the result of the corruption. Again the challenge is to identify the kind of corruption.

One of the techniques employed in Receiver Autonomous Integrity Monitoring (RAIM) uses the overdetermined PVT solution to detect the presence of corruption and mitigate the effect.



3.4.2.3 Weighing pseudoranges

C/N_0 can be used to weigh the pseudoranges in the PVT computation. A satellite with a high C/N_0 gets a high weight, a satellite with a low or rapidly fluctuating C/N_0 gets a low weight. The net result is a more robust PVT solution. Depending on the characteristics of the interference, the influence can be reduced.

Another quantity to use as weight factor is the pseudorange noise variance derived from the code minus carrier combination. When the integrated carrier phase is expressed in length units ('carrier range'), its average change in time is to a large extent similar to the average change of the pseudorange in time (with the exception of the ionosphere delay: it advances the carrier range and delays the pseudorange). Pseudorange noise is orders of magnitude higher than carrier range noise, hence the noise in the difference is dominated by pseudorange noise.

The difference of pseudorange and carrier range is therefore constant in time to the pseudorange noise and twice the ionosphere delay. Usually the ionosphere delay changes very slowly in time, hence for short (in the order of a few minutes) time spans the difference can be assumed to be a constant with pseudorange noise added. The RMS noise amplitude is represented by the variance of a moving average filter with a time constant in the order of a few minutes (100 sec is often used). Pseudorange noise is composed of the noise in the RF signal, receiver electronics noise, and if present multipath and/ or EMI. Thus the noise amplitude is also a measure for the amount of corruption.

3.5 High sensitivity GPS

In a weak signal environment such as inside parking buildings, in the urban canyon or under heavy foliage it may be required to increase the sensitivity of the receiver in terms of acquisition and tracking. As explained earlier knowledge of the 50bps navigation bit reversal can extend correlation times well beyond the navigation bit duration of 20msec and will increase the success on acquisition or the robustness of tracking.

Assisted GPS (AGPS) is a technique whereby the 50bps navigation message is delivered via an alternative path, e.g. via cell phone. When the receiver position and clock error are known reasonable accurately (e.g. from a previous session) it is possible to estimate the sign and moment of the bit reversal. Coherent integration time can then be extended to e.g. 600msec, which improves the post-correlator signal to noise ratio by ~18dB referred to 10msec integration time. This gives a considerable improvement in both acquisition and tracking performance.



Inertial aiding of the carrier tracking loops allows a decrease in the loop bandwidth. This results in reduced range noise and an increase in sensitivity of ~14dB.

Increasing the sensitivity of the acquisition and tracking processes has the added advantage of a similar increase in robustness to jamming.



4 EMI effects, detection and mitigation

In the previous chapter the architecture of a typical low cost GPS receiver has been described from antenna to PVT solution. In this chapter the chain from antenna to PVT solution is walked through again but now with the emphasis on the detrimental effect of EMI and possible ways to detect the presence of EMI. Mitigation inside the receiver of the effect of EMI is not the primary objective of the study, but will be mentioned where applicable.

It is emphasized that the effects of EMI, the detection and mitigation are limited to the ‘isolated’ receiver. Integration of the receiver data with other systems data can be advantageous for further detection and mitigation, but is not the subject of this investigation.

4.1 Antenna

Due to the short distance inside the OBU between antenna and receiver a passive antenna is assumed. The proper functioning of the antenna is to a large extent indifferent to EMI. The antenna does not offer means to detect EMI. Its design however can mitigate effects of EMI in the following way.

- Out of band EMI: the antenna should resonate on the L1 frequency and have a bandwidth in the order of 2MHz.
- In band EMI with non-RHCP components (and multipath reflections): the ratio of RHCP sensitivity to non-RHCP sensitivity should be high, in the order of 20dB.
- In band EMI from transmitters at low elevation (and multipath reflections): the antenna should be insensitive below an elevation of 5 deg. Preferably it has a radiation diagram as given in figure 2.

Table 1. EMI matrix antenna

Type of EMI	Effect	Detection	Mitigation by antenna
Jamming	none	none	Out of band: yes
Meaconing, spoofing	none	none	none

4.2 Front end

The proper functioning of the front end can be disrupted by high levels of EMI. The input of the LNA can even be permanently degraded by very high levels of EMI (~10dBm, [2]).

The actual bandwidth of the antenna will be much larger than 2MHz. In order to reject out of band EMI and reduce the chance of overload of the input of the LNA, a band pass filter should be present between antenna and LNA with a bandwidth of 2 MHz, a steep roll-off and a low noise figure. An interdigital cavity filter can be designed to meet these requirements, it needs



however careful tuning and is bulky and expensive. Therefore a Surface Acoustic Wave (SAW) filter with somewhat less favorable properties is the next best alternative. A microstrip hairpin filter on a substrate with a high dielectric constant may also offer a reasonable alternative.

The input of the LNA should be protected by a power limiter (e.g. back to back PIN diodes) to prevent overload or destruction by EMI. It has the added advantage of reducing the power in pulse EMI to a level where it has little effect on the operation of the receiver.

The VGA should have a sufficiently large gain range (in the order of 50dB) to accommodate reasonable amounts of EMI power.

The A/D converter should offer at least 1,5 bit, but preferably 2 or 3 bits in order to increase performance with an effective AGC loop. The AGC value is a good indicator for EMI exceeding the thermal noise within the passband of the front end.

The AGC loop characteristics change in time, mainly due to temperature variation sensitivity of the gain of the amplifiers (~3dB has been observed). The loop can be calibrated by injection of known amplitude signals into the front end at regular intervals. This feature complicates the design of the front end, but allows detection of EMI with a power of only a few tenths of a dB above the thermal noise power level [3, 4].

The AGC value is always available, even with the receiver being jammed to a level where no acquisition or tracking is possible. This is an advantage when AGC is used to detect EMI. Under normal operation (no EMI) the thermal noise dominates the satellite signal by tens of dB's. Hence the distribution of the AGC bits is Gaussian (for a 2-bit converter the normal distribution will be 16.35 % 33.65 % 33.65 % 16.35 %). When CW is present, the distribution in the outermost bins will be higher. This offers a way to detect CW jamming. When high power jamming drives the AGC into saturation, again the distribution of samples in the outermost bins will be higher, and again offer a way to detect high power jamming.

The power required to have the receiver captured by meaconed or spoofed signals is only slightly higher than the satellite signal. The front end has no means to detect the presence of this interference unless the meaconed or spoofed signals are significantly higher. A high AGC value will warn for this.

The range between a moving vehicle and jammers/ meaconers/ spoofers at a fixed location will vary in time. This will cause the AGC value to vary proportionally to the range rate of change.



The AGC variation due to the range rate of change between a moving vehicle and a satellite is considerably less. Hence the AGC rate of change (AGC-dot) is an indicator for a fixed location jammer, meaconer or spoofer.

In table 2 below the results of this subsection are summarized.

Table2. EMI matrix front end

Type of EMI	Effect	Detection	Mitigation by front end
Broadband noise	saturation	AGC, bit distribution, AGC-dot	Out of band: yes
Narrowband – low power	none	Bit distribution	none
Narrowband – high power	saturation	AGC, bit distribution, AGC-dot	Out of band: yes
Pulse	saturation	AGC-dot	PIN diodes
Meaconing, spoofing	none	AGC if high, AGC-dot	none

Remark: interferers can be located (and eliminated) using a network of ‘AGC receivers’ [11].

4.3 Baseband processor

The power level of meaconing or spoofing signals at the base band process input needs only to be slightly higher than the satellite signal in order to capture the baseband processor. The baseband processor has no means to detect capture by spoofing or meaconing. Therefore in the following subsections only jamming is elaborated.

4.3.1 Code acquisition

Since code acquisition typically requires a C/N_0 ratio which is 10dB higher than for tracking, acquisition is a weak link in a GPS receiver. All kinds of EMI may leak through the base band process. Broadband noise will be added to the thermal noise and corrupt the (integrated) I and Q values, narrowband interference may be reduced by the carrier and code correlation process but may also corrupt I and Q when the frequency band happens to coincide with a spectral code peak. The result is either a reduced chance on acquisition or no acquisition at all.

It is emphasized that the integrated I and Q values are formed in the post correlation domain. The I- and Q signals contains therefore the despread satellite signal, the spread thermal noise, and the spread jamming. The thermal noise is equally divided over I and Q, the distribution of the jamming in I and Q depends on the type of jamming. So, the information about the satellite signal, thermal noise and jamming power is contained in the I and Q values of the channel



correlating with PRN and the I and Q values of the channel correlating with a non-existent PRN (and the pre detection integration times).

The satellite signal value and the combined noise and jamming power levels are calculated according 3.3.2.4.

In [2] the acquisition process of one GPS receiver is determined for various kinds of jamming in terms of noise power *increase*, Signal to Noise Ratio (SNR) *decrease*, and acquisition success.

The relevant details for the acquisition process are:

- Satellite signal level: -130dBm
- Coherent integration time: 10msec
- Detection threshold: $6.45 * \text{noise standard deviation}$ (the noise standard deviation is calculated from a number of successive noise measurements Q_N)

It was shown that this receiver reaches 100% acquisition success in the absence of jamming.

Table 3 below gives an overview of the effect of jamming on this receiver for various types and power levels of jamming. The right most power number in each column gives the jamming power relative to the satellite signal level (J/S).

Table 3. Average values for noise power increase, SNR decrease, and acquisition success due to the effect of jamming

Type	Noise power increase @ J/S	SNR decrease @ J/S	Acquisition success @ J/S
CW	4dB @ 30dB 1.4dB @ 10dB	10dB @ 30dB 3dB @ 10dB	Correct acq < 10dB False acq > 15dB
Swept CW	2.3dB @ 30dB 1.1dB @ 15dB	5dB @ 30dB none @ 15dB	Correct acq < 15dB False acq > 20-25dB
BB noise	Very little < 60dB	2dB @ 60dB 1.5dB @ 15dB	Correct acq < 15dB No acq > 20dB
Pulse	None < 90dB	None < 90dB	Always correct acq
AM	2dB @ 30dB 1dB @ 15dB	7dB @ 30dB 3dB @ 15dB	Correct acq < 15dB False acq > 25-30dB
FM	2dB @ 30dB 0.8dB @ 20dB	0-7dB @ 30dB 0dB @ 20dB	Correct acq < 20dB False acq > 35dB

Although the table presents the results for just one receiver, the numbers and trends are indicative for the class of low-cost receivers. It is clear that both noise power increase and SNR decrease can be used to detect the presence of some types of jamming. Unfortunately the effects of the various types and levels of jamming on the I and Q values for signal and noise has not



been studied in [2]. A follow-up study may show that the I and Q values for signal and noise allow a better detection/ characterization of jamming.

The I and Q amplitudes depend also on the integration time T_{int} . Therefore the actual integration time has to accompany the I and Q values.

The I and Q values (and derived quantities) are always available, even with the receiver being jammed to a level where no acquisition is possible. This is an advantage when they are used to detect EMI.

The frequency domain search (Fourier transform of the signal samples during one or more code chips) allows detection of narrowband interference, even at low power levels. Interference can be removed by zeroising the peak in the spectrum. It requires however at least a 10bit ADC in the FE.

4.3.2 Code- carrier tracking

4.3.2.1 Loss of lock

When the jamming power is high enough it will cause loss of tracking of one or more channels, forcing the channel(s) to re-enter acquisition (with ~10dB more required C/N_0). In [6] the required interference power to cause loss of lock is calculated for a typical receiver. The signal is estimated to be -127dBm, the thermal noise -111 dBm. The graph in figure 9 summarizes the results as a function of the interference bandwidth.

The carrier tracking loop is the critical loop: it is more sensitive to noise/ jamming, and it aids the code tracking loop. Therefore the carrier tracking loop performance is determining the baseband process performance under jamming.

For very narrowband jamming (CW jamming) 6dB worst case, 14dB average jamming above the signal is sufficient to cause loss of carrier lock. These values are below the thermal noise threshold of 16dB above the signal. It is emphasized that under narrowband jamming usually only one channel is affected at the same time, and only when the jammer frequency happens to coincide with a code spectral peak.

The jamming resistance increases to a value of 35dB for broadband noise, well above the thermal noise threshold.

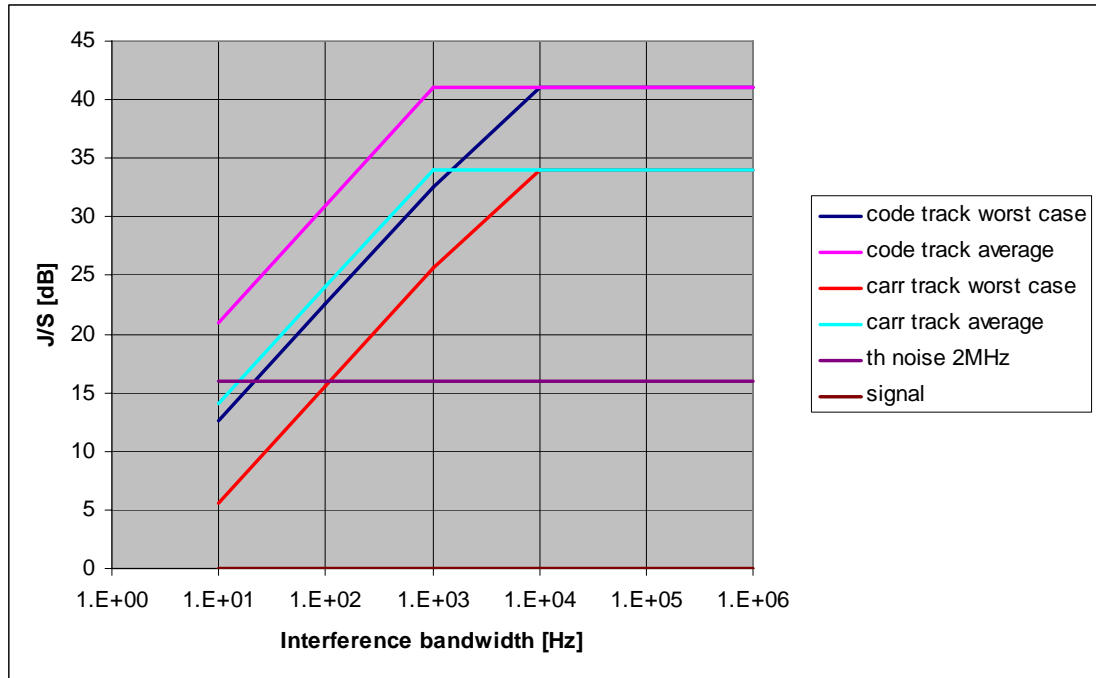


Figure 9. Required interference power for loss of lock for a typical receiver

4.3.2.2 The role of C/N₀

When no loss of lock occurs, jamming will affect the performance of the tracking loops which will result in a pseudorange error. The C/N₀ ratio is often used as the bridge between interference/ jamming and pseudorange degradation. In [3] and [7] various ways have been described to derive C/N₀ from (early, prompt, late and noise) I and Q values, some good and some bad. The good methods allow reliable estimation of the pseudorange degradation. Therefore it must be known which way has been implemented in a receiver before it can be used to detect/ characterize jamming and pseudorange degradation.

The relation between C/N₀ and pseudorange degradation is receiver specific, no general guidelines can be given. The receiver manufacturer must supply this data. Once this data is available, C/N₀ can be used on one hand to detect and characterize jamming, and on the other hand be used as pseudorange weight factor (or pseudorange exclusion threshold) in the conversion from pseudoranges to receiver PVT.

4.3.2.3 Correlator output power

The Correlator Output Power (COP) is defined in [8] as:

$$COP = (I_p^2 + Q_p^2) / \text{Noise},$$

where I_p and Q_p are the 1msec averaged prompt correlator signals, and Noise is the receiver specific expected noise floor.



‘Carrier Phase Vacillation’ $\dot{\Phi}$ is defined in [8] as the 1sec time average of the absolute values of $\{\Phi(i) - \Phi(i-1)\}$ where i is the 1msec epoch index, and $\Phi(i) = \arctan\{I_p(i) / Q_p(i)\}$. In [13] the usability of the COP, its variance (COP- σ) and $\dot{\Phi}$ is investigated to detect and characterize jamming. It is concluded that all three metrics perform well for the purpose.

4.3.2.4 Correlator output signals

The early, prompt, late, and noise integrated I and Q signals together with the integration time form the basis for the calculation of C/N_0 , COP, COP- σ , and $\dot{\Phi}$. Surprisingly, no articles have been found which bridge detection and characterization of jamming on one hand, and the degradation of pseudoranges at the other hand. It might be advantageous to investigate this relation for typical low cost GPS receivers.

4.3.2.5 Discriminators and filters

The way in which the code- and carrier loop discriminators and filters are implemented defines together with the integration time the resistance (and mitigation) of the channel against jamming. Filter tracking error is an indicator for the presence of EMI. Many implementation variants exist, the implementation is usually the manufacturers’ proprietary information. Hence no data can be supplied in the framework of this study. Actual tests on a specific receiver may gain insight into the resistance to jamming of discriminators and filters.

4.4 Navigation processor

4.4.1 The role of C/N_0 revisited

As has been stressed earlier the C/N_0 , if correctly implemented, is a good indicator for the presence and classification of jamming. This is especially the case for one of the most detrimental forms of jamming: CW. The coincidence of the CW frequency with a spectral peak in the signal spectrum causes a sharp drop in C/N_0 , as illustrated in figure 10 below from [5].

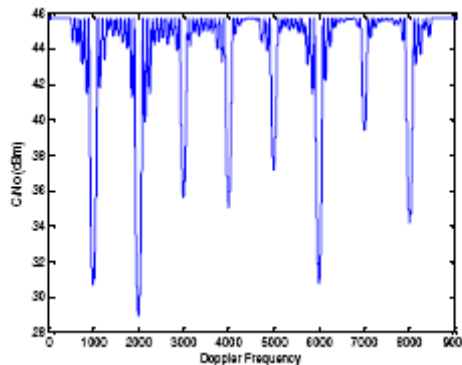


Figure 10. Calculated value of C/N_0 with a fixed frequency CW signal and the satellite Doppler changing from 0 to 10kHz



The equidistant troughs indicate the presence of CW jamming, the frequency difference between the troughs indicates a fixed frequency jammer or a swept CW jammer.

C/N_0 can also be used to (de)weigh pseudoranges in the PVT calculation. The relation between C/N_0 and pseudorange degradation needs to be established for the specific receiver.

4.4.2 Code minus carrier combination

The carrier phase lock mechanism usually breaks at a carrier phase error in the order of 45deg, which is 2.5cm when expressed in length units. This is the maximum error in a carrier phase tracking channel. The code tracking (pseudorange) error however can be hundreds of meters. The difference of pseudorange and integrated carrier range ('code minus carrier') contains the pseudorange error, the carrier range error, the so-called carrier phase ambiguity which is a constant value as long as the phase loop remains in lock, and the ionospheric divergence [6]. The code minus carrier combination is therefore a good indicator of pseudorange degradation. This degradation however can also be caused by multipath reflections and/ or atmospheric disturbances.

The variance of the code minus carrier combination can be used to (de)weigh pseudoranges in the PVT calculation. Due to the ionospheric divergence the time segment in which the variation is calculated is usually limited to 100sec.

A rapidly diverging code minus carrier combination with low noise may be an indication of a spoofed signal.

4.4.3 Data coherence

The GPS receiver usually outputs raw data such as pseudoranges, integrated carrier phases, Doppler frequencies and C/N_0 values once each second. The pseudorange rate of change, delta carrier range and Doppler expressed in meters should be identical to their accuracy limits. Delta carrier is the most accurate at the sub-dm level, as long as the channel loop remains in carrier tracking. Pseudorange rate of change can be in error by meters, Doppler by tenths of meters. This coherence can be used to detect a not too sophisticated spoofer.

Abnormal rate of change of quantities as AGC, C/N_0 can also indicate the presence of a fixed location spoofer from a moving vehicle. Table 4 below [9, 10] summarizes spoof countermeasures. They all rely on some kind of data coherence.



Table 4. Countermeasures against spoofing

Test statistic	Detection of spoof	Quantity	Limitations
Absolute signal power	Not consistent with thermal noise	AGC	Environment Accuracy of AGC measurement
Signal power rate of change	Rapidly varying	AGC-dot	Not for own vehicle based spoofer
Spoofed C/N0 on all channels	Identical values, not consistent with sat elevation	C/N0, Elevation	Smart spoofer; realistic C/N0 on each channel
Delta carrier	Not consistent with satellite/ user geometry	Carrier phase	Channel in carrier tracking
Pseudorange rate of change	Not consistent with delta carrier	Pseudoranges	High multipath
Doppler	Not consistent with delta carrier	Dopplers	None
Raw data rate of change	Large jumps when switching from normal to spoof	Raw data	None
Position/ velocity residuals (RAIM)	Large residuals in one or more channels	Pseudoranges, Dopplers	Overdetermined number of observations
Navigation data rate of change	Data not consistent with earlier collected data or AGPS data	Almanac, Ephemeris, clock correction data	No trusted navigation data available
Satellite constellation	Not consistent with current user position/ time	Ephemeris data, estimated own position, time	No trusted navigation data available
Time comparison	Calculated GPS time not consistent with other time source	Own PVT, external time source	Integration with independent system required
Sanity check	Compare horizontal velocity with compass, accelerometer	Own PVT, external compass, accelerometer	Integration with independent system required



4.4.4 Receiver Autonomous Integrity Monitoring

RAIM is a technique to detect and remove erroneous pseudoranges from the position solution. It can only be applied when 5 or more satellites are being tracked. It relies on the range residuals in the position solution to have 'normal' values, usually in the order of a few meters. Larger than normal range residuals can be caused by one or more degraded pseudoranges. With more than 5 satellites in track subsets of 5 satellites can be formed by excluding one (or more) satellite(s) from the position solution. A subset which has normal range residuals points to the excluded satellite(s) being degraded.

Pseudorange degradation can be the result of jamming/ spoofing. It can also be caused by multipath reflections and/ or weak signals. RAIM should therefore be used together with another jamming/ spoofing technique to identify its origin.

4.4.5 Spoofing and Meaconing

Spoofed or meaconed signals can be transmitted from a fixed location or from a transmitter inside the vehicle. For a fixed location transmitter the countermeasures given in section 4.4.3. apply.

The signals from an in-vehicle transmitter must override the satellite signals by at least 3dB [9]. Detection of the transmitter in the same way as in-vehicle jammers is a possibility.

An in-vehicle transmitter may spoof a stationary scenario. The majority of countermeasures given in section 4.4.3 will not apply. Only 'time comparison' and 'sanity check' can detect spoofing or meaconing.

When the in-vehicle transmitter spoofs a moving scenario most of the countermeasures apply.

4.5 Integration with other sensors

Although it is not within the scope of this investigation, integration of GPS with other sensors can be beneficial in several fields. In section 3.5 it has been mentioned that AGPS and integration with inertial sensors increases the sensitivity of the receiver (weak signal environment), and at the same time increase the robustness of the receiver for jamming. AGPS also enables consistency checks on the 50bps navigation data, and time comparison (see table 4 above). Inertial sensors allow a sanity check on the position and velocity data. Hence AGPS and integration with inertial sensors increase detection success of meaconing and spoofing.



5 Low cost receiver output for EMI detection

In [4, 11] a very effective technique (Jamming to Noise Meter) is described to detect EMI in the Front End. The technique is applicable for low cost receivers but requires a re-design of the FE. Receivers with this technique may become available in near future. The technique relies on an optimal (2-bit) ADC and optimal implementation of AGC. For receivers without this technique the AGC control output and the ADC bit distribution are an alternative.

Noise power and C/N_0 are determined at the Baseband stage and are, when properly implemented, good indicators for the presence of EMI. In-phase and Quadrature signals are available for both a channel in acquisition as in tracking. This is an advantage over C/N_0 which is only available with the channel in tracking.

Correlator output power and derived quantities are again good EMI indicators, for a channel in track.

The input to the navigation processor: pseudoranges, integrated carrier phases, Dopplers and 50bps navigation data (almanac, ephemeris and satellite clock parameters) offer many ways to detect the presence of EMI.

Finally the PVT calculation itself offers the possibility to detect (RAIM) and mitigate (exclusion or de-weighting) the effects of EMI.

Not all low cost receivers output the above quantities, or have the processes implemented. In table 5 some low cost chip sets are investigated on these aspects.

Table 5. Output of EMI detection quantities

Stage	Detection quantity	SiRF-II	SiRF-III	Antaris 4	u-blox 5
FE	AGC	Y	Y	Y	Y
FE	Bit distribution	N	N	N	N
BB	noise power	N	N	Y	Y
BB	C/N_0	Y	Y	Y	Y
BB	COP etc	N	N	N	N
BB	I, Q, T_{int}	Y?	Y	N	N
BB	tracking loop errors	N	N	N	N



Stage	Detection quantity	SiRF-II	SiRF-III	Antaris 4	u-blox 5
BB	Pseudorange	Y	Y	Y	N
BB	(integrated) carrier phase	Y	Y	Y	N
BB	Doppler	Y	Y	Y	N
BB	50bps	Y	Y	Y	N
Nav	Sat excl	N	N	Y	Y
Nav	P, V residuals	N	N	Y	Y

It is my belief that implementation of the above detection quantities by the manufacturers is feasible.



6 Conclusion and recommendations

6.1 Conclusions

It is concluded that a GPS receiver is vulnerable to EMI. Broadband noise and CW signals pose the greater threats.

Jamming is simple, it takes little money and intelligence to implement. With a well designed receiver most types of jamming can be detected, only broad band noise with sufficient power can not be mitigated.

Meaconing is more sophisticated, but should be feasible for the advanced amateur.

Spoofing is the most complicated and expensive to realize. It requires a deep knowledge and sophisticated equipment. It is expected however that within 5 – 10 years techniques such as meaconing and spoofing will become available to the mass market. The detection success of meaconing or spoofing can be considerable increased by integration of the GPS receiver with other sensors. AGPS and inertial integration have been mentioned as examples.

In detail the following technical points are concluded.

6.1.1 Antenna

- The GPS receiver antenna offers no means to detect EMI, but a well designed antenna will mitigate some of the effects of EMI.

6.1.2 Front end

- The first Low Noise Amplifier is vulnerable to high levels of EMI. Very high power can even destroy the amplifier.
- A multibit front end allows the implementation of Automatic Gain Control (AGC), which is an efficient indicator for the presence of EMI. The AGC signal is available regardless of the state of the receiver: searching or tracking.
- A calibrated AGC allows detection of EMI with a power of a few tenths of a dB above the thermal noise level. This feature however complicates the front end design.
- A high AGC value indicates the presence of a jammer/ meaconer or spoofer, either in vehicle or at a fixed location. Variations in the AGC level indicate fixed location jammers, meaconers or spoofers.
- The front end digital output bit bin distribution offers the possibility to detect the presence of narrow band (CW) EMI.

**6.1.3 Base band processor, acquisition state**

- A receiver channel in acquisition is more vulnerable to EMI by ~10dB than a channel in tracking.
- A CW jammer to signal ratio of 15dB (which is well below the thermal noise threshold) can already deny acquisition or provide false acquisition. Usually this occurs on one channel at a time only.
- Broadband noise at 20dB above the signal can deny acquisition or provide false acquisition. This will happen on all channels, unless they are already in tracking mode.
- Integrated values of the in-phase and quadrature branches provide information on the presence and classification of EMI. The I and Q values are available regardless of the state of the channel: acquisition or tracking. Usually they are not provided in the output of the receiver.

6.1.4 Base band processor, tracking state

- The I and Q values and the integration time are used to calculate C/N_0 and noise power. C/N_0 is always a receiver output for all channels in tracking mode. Noise power is sometimes also provided. Both figures provide information on the presence and classification of EMI.
- The frequency domain search in combination with a 10bit ADC allows narrowband EMI detection and mitigation. At this moment in time this technique is too sophisticated for low cost GPS receivers.
- A carrier tracking loop is more sensitive to EMI by ~10dB compared to a code tracking loop, and is therefore the weaker link in the tracking process.
- A CW jammer to signal ratio of 14dB can already cause carrier loop loss of lock. About 24dB is required to cause code loop loss of lock.
- A broadband noise jammer to signal ratio of 35dB can cause carrier loop loss of lock.
- Depending on its implementation, C/N_0 can be an indicator of the presence and classification of EMI.
- Both correlator output and code and carrier loop tracking errors can be indicators for the presence and classification of EMI.

6.1.5 PVT calculation

- Both the code minus carrier combination and C/N_0 can be used to (de)weigh the ranges in the PVT computation.
- Delta pseudorange, carrier phase, Doppler, and 50bps data consistency can be used to detect the presence of meaconing and spoofing.



- RAIM can be used to detect erroneous range measurements and to (de)weigh or exclude them from the position solution.

6.2 Recommendations

A low cost GPS receiver is an important component in the On Board Unit (OBU). Most, if not all, low cost GPS receivers have not been designed to operate under EMI, meaconing or spoofing conditions. They do however output quantities such as C/N_0 , which can be used to detect the presence of EMI and to mitigate the negative effects of EMI. Adaptations to their design allow improved detection, classification and mitigation of unintentional interference, jamming, meaconing, and spoofing.

Below a number of adaptations are recommended. Some of them may already be implemented in receivers. It is believed that most of these adaptations are simple to implement.

Recommendations with respect to EMI detection are summarized first. The availability of Automatic Gain Control (AGC), noise and correlator power, C/N_0 ratio, and raw data are emphasized. Algorithms using detection quantities can be implemented either within the PVT calculation or elsewhere in the OBU and signal the presence of detrimental signals to the vehicle driver. They are followed by recommendations with respect to mitigation. These adaptations should be implemented within the receiver.

6.2.1 Recommendations with respect to EMI detection

- To allow implementation of AGC the receiver front end output should deliver the digitized signal at least with 1,5 bit, preferably 2 bit resolution. The AGC control signal is an indicator for the presence of EMI, meaconing, or spoofing, and should be available as output signal.
- AGC calibration complicates the front end design but offers an improved possibility of EMI detection.
- A high sensitivity baseband processor may only be affected by EMI which is well above the thermal threshold. Detection of EMI by AGC is then feasible.
- The receiver should output C/N_0 ratio and noise power, and preferably should output correlator power. The manufacturer should provide detailed information of the implementation of noise and correlator power determination, and C/N_0 calculation. Alternatively I and Q, and integration time values could be made available in the receiver output for more robust EMI detection and classification.



- The receiver output should include raw data (pseudoranges, integrated carrier phases, Doppler and navigation data) to allow detection of jamming, meaconing and/ or spoofing by data consistency checks.
- Integration with other sensors increases robustness against jamming and increases the detection success of meaconing and spoofing.

6.2.2 Recommendations with respect to EMI mitigation

- The GPS antenna should resonate on the L1 frequency. A low noise, narrow band (~2MHz) filter should be added in front of any Low Noise Amplifier to suppress out of band EMI. The antenna should be insensitive to non-right hand circular polarized signals. The gain pattern should be optimized for the vehicle.
- The LNA directly downstream of the antenna element should be protected for high EMI levels, e.g. by back to back PIN diodes. This offers the added advantage of suppression of high energy pulsed EMI.
- The AGC range should be sufficient (~ 50dB) to accommodate reasonable amounts of EMI.
- RAIM should be implemented as a part of the PVT computation. Code minus carrier combinations and/ or C/N_0 should be used to (de)weigh range data.

This investigation has used data of a limited number of GPS receivers, not necessarily in the low cost segment. The data may therefore not be fully representative for the class of low cost receivers.

Additional tests in a laboratory environment on a limited number of low cost receivers will establish their actual vulnerability to the various kinds of EMI. This will provide insight into the real behavior of this class of receivers, and will provide a better understanding of how these receivers can be improved (and what can be asked from the manufacturers) in terms of vulnerability to EMI, meaconing and spoofing. The proposed tests will produce threshold values for proper operation under EMI. With the threshold values a plan for initial and continued EMI tests on the GPS component inside OBU's can be drafted.

A research software receiver is based on a high quality hardware front end, with the baseband process implemented in easy to modify software. Such a receiver can be configured to mimic a low cost receiver. It allows to investigate the effects of EMI at places which are not accessible on the actual receiver, e.g. the integrated I and Q values. It is recommended to add such a receiver to the laboratory tests.



Referred publications

1. Vulnerability of GNSS for ABvM application, D. van Willigen, 17 August 2007.
2. Study of Interference Effects on GPS Signal Acquisition, Sameet Mangesh Deshpande, July 2004
3. Understanding GPS Principles and Applications, 2nd edition, Elliott D. Kaplan, Christopher J. Hegarty, 2006
4. Simple Techniques for RFI Situational Awareness and Characterization in GNSS Receivers, Phillip W. Ward, January 2008
5. A Novel Approach in Detection and Characterization of CW Interference of GPS Signal Using Receiver Estimation of C/N0, Balaei, A.T., Dempster, A.G., Barnes, J., 2006
6. Global Positioning System: Theory and Applications, Bradford W. Parkinson, James J. Spilker, 1996
7. Effect of Partial-Band Interference on Receiver Estimation of C/N0: Measurements, Jeffry T. Ross, Joseph L. Leva, Shawn Yoder, January 2001
8. GPS Receiver Autonomous Interference Detection, Awele Ndili, Dr. Per Enge, April 1998
9. Countermeasures for GPS Signal Spoofing, Hengqing Wen, Peter Yih-Ru Huang, John Dyer, Andy Archinal, John Fagan, September 2005
10. Interference Effects on GPS Receivers in Weak Signal Environments, Nyunook Kim, January 2006
11. RFI Situational Awareness in GNSS Receivers: Design Techniques and Advantages, Phillip W. Ward, April 2007



Other relevant publications

A Preventative Approach to Mitigating CW Interference in GPS Receivers, Balaei, A.T., Motella, B., Dempster, A.G, 2006

Automatic Gain Control (AGC) as an Interference Assessment Tool, Frederic Bastide, Dennis Akos, Christophe Macabiau, Benoit Roturier, 2003

Effect of Partial-Band Interference on Receiver Estimation of C/N0: Theory, John W. Betz, January 2001

GNSS Interference Detection and Localization using a Network of Low Cost Front-End Modules, Jonas Lindström, Dennis M. Akos, Oscar Isoz, Marcus Junered, September 2007

GPS Interference detected in Sydney-Australia, Balaei, A.T., Motella, B., Dempster, A.G, December 2007

GPS Signal to Noise Measurement in Weak Signal and High Interference Environments, Paul D Groves, September 2005

GPS Spoofing Countermeasures, Jon S. Warner, Roger G. Johnston, December 2003

On the Interference Mitigation Based on ADC Parameters Tuning, Simone Savasta, Beatrice Motella, Fabio DAVIS, Riccardo Lesca, Davide Margaria

Radio Interference Effects on Commercial GNSS Receivers Using Measured Data, Thomas Jost, Christian Weber, Cecil Schandorf, Holmer Denks, Michael Meurer, 2008

Receiver Autonomous Interference Detection, Awele Ndili, Dr. Per Enge, 1996



Appendix A Uncorrelated signals

During this investigation some facts have become available which are not directly linked to the investigation but which may be of importance for the project ABvM. These ‘uncorrelated signals’ are given below.

- What is effect of addition of EGNOS/ Galileo/ Glonass.
- Multiple freq: better resistance to jamming (code or codeless), better spoofing/ meaconing detection (multiple system/ multiple freq coherence)
- Position plausibility checks (e.g. not being located in/above open water areas). Same could be true for the calculated height. Since the vehicles will be on the ground, the GPS height for a given position should be close to the ground height above the WGS’84 ellipsoid.
- RF power without antenna cover should be <1dB less than RF power with antenna cover (sky is ‘colder’ than cover)
- Use of differential signals as transmitted by e.g. FM radio channels. Information may include the health of satellites and updated ephemeris data.
- One final comment: SiRF-II did not use the same process as SiRF-III with one small exception: both receivers use a fast Fourier transform as part of their search algorithm, and that of necessity uses data sampled and stored. For tracking, SiRF-II used traditional correlators while SiRF-III uses the algorithm I discussed elsewhere, which Russel quoted.
From: Carl - SiRF Customer Support.
- A high precision local (atomic) clock inside the OBU
- Null-steering antennas