GNSS interference detection

ERIK AXELL

FOI-R--3839--SE
ISSN 1650-1942 February 2014

Erik Axell

GNSS interference detection

Titel	GNSS interferensdetektion
Title	GNSS interference detection
Rapportnr/Report no	FOI-R--3839--SE
Månad/Month	February
Utgivningsår/Year	2014
Antal sidor/Pages	37 p
ISSN	1650-1942
Kund/Customer	Försvarsmakten
Forskningsområde	4. Informationssäkerhet och kommunikation
FoT-område	Ledning och MSI
Projektnr/Project no	E36044
Godkänd av/Approved by	Christian Jönsson
Ansvarig avdelning	Informations- och Aerosystem

Sammanfattning

Användandet av Global Navigation Satellite System (GNSS)-mottagare, t.ex. Global Positioning System (GPS), är vitt spridd i samhället idag. GNSS-mottagare används för navigering inom många säkerhetskritiska områden såsom marin, flyg och polis/räddningstjänst, men även för tidssynkronisering i viktiga infrastrukturella tillämpningar som mobiltelefonisystem, elnät och finansiella system. Med hög användning och hög tillit, kommer också en sårbarhet mot avbrott p.g.a. interferenser, störsändning eller vilseledning. Ett första steg för att motverka effekterna av störsändning är att upptäcka störaren och att varna användaren för att positionslösningen är otillförlitlig.

Huvudmålet med detta arbete är att utvärdera olika sätt att detektera störsignaler i de frekvensband som används av GNSS. Målet med arbetet har varit att utvärdera möjligheterna att upptäcka en okänd störsignal. Därför har fokus varit att utvärdera detektorer som inte kräver någon kunskap om störsignalens specifika egenskaper. Utvärderingarna i detta arbete har gjorts baserat på mätningar av riktiga GPS-signaler och störsignaler. I rapporten visas att detektorer som baseras på mottagen energi, *automatic gain control* (AGC), och mottagarens uppskattade *carrier-to-noise ratio* (C/N_0) kan användas för att upptäcka många olika typer av störsignaler från smalbandiga (CW) till bredbandiga (> 20 MHz) signaler. Prestanda för de olika metoderna beror på tillämpningen och dess krav, såväl som på hårdvaran och möjligheten att justera parametrar såsom beslutströskel och detektionstid.

Energidetektion är en enkel metod som ofta fungerar bra. För att beräkna den mottagna energin måste man i princip ha tillgång till rådata i mottagaren, vilket i allmänhet inte är möjligt i en kommersiell produkt. AGC-värden kan finnas tillgängliga i större utsträckning, och därför kan en detektor baserad på AGC vara ett bra alternativ till energidetektion, med liknande egenskaper. Naturligtvis är AGC-värden oundvikligen kvantiserade, och därför förloras viss prestanda jämfört med att använda rådata.

C/N_0–baserade detektorer är i allmänhet inte lämpliga att använda i tillämpningar där den mottagna signalstyrkan från satelliterna normalt varierar, t.ex. i dynamiska scenarier i stadsmiljö. Detta beror på att dessa detektorer inte kan skilja mellan en minskad signalstyrka i GNSS-signalen och en ökad störsignal.

Nyckelord: GPS, GNSS, detektion, störsändning, interferens

Summary

The use of Global Navigation Satellite System (GNSS) receivers, such as the Global Positioning System (GPS), is wide spread in the society today. GNSS receivers are used for navigation in many safety critical sectors, such as maritime, aviation and first responder applications, but also for timing synchronization in important infrastructural applications such as the power grid, mobile telephony systems and financial investment systems. With the wide spread usage and high reliance of GNSS, also comes vulnerability to outages due to interference, jamming and spoofing. The first step towards mitigating the effects of jamming is to detect that there is a jammer and if the delivered GNSS position and time solution is unreliable.

The main goal of this work is to evaluate different approaches for detecting interference signals in the GNSS frequency bands. The focus of the evaluation has been on detectors that makes no assumption on the jammer signal characteristics. The evaluations in this work are based on measurements of authentic GPS and jamming signals. It has been shown that detectors based on received energy, automatic gain control (AGC) levels, and receiver carrier-to-noise (C/N_0) estimates are able to detect many different types of signals ranging from narrow band (continuous wave) signals to wide band (>20 MHz) signals. The performance of the different methods depends on the application and its requirements, as well as on the hardware and the possibility to change parameters such as the decision threshold and detection time.

Energy detection is a conceptually simple detector that often performs very well. However, to compute the energy, one essentially needs to have access to the raw IF samples. These are generally not available in an off-the-shelf product. AGC values could be available and therefore an AGC based detector could be a good alternative to the energy detector, with similar properties. Of course, the AGC gain is necessarily quantized, and as such some detection performance is lost as compared to dealing with raw IF data.

C/N_0–based detectors in general are not suitable for applications where the received satellite signal strength normally varies, such as dynamic scenarios in urban environments. The reason is that these detectors cannot distinguish between an increased noise-plus-jammer-power and a decreased desired signal power.

Keywords: GPS, GNSS, detection, jamming, interference

1 Introduction

The main application for the work herein is a soldier (or first responder) positioning system, with a focus on urban operations which also includes transitions between outdoor and indoor environments. Currently, such systems are mainly based upon stand-alone GPS receivers. For these systems it is of crucial importance to have accurate information about if the position information provided by the GPS receiver is reliable or not. In addition, it is important, if the position is unreliable, to identify if the problem is caused by jamming or interference so that appropriate actions can be taken. Furthermore, soldier positioning systems based on multisensor approaches are under development and such systems are expected to become available on the market within a few years.

This work is relevant also for the development of future multisensor positioning systems for soldiers, small unmanned aerial/ground vehicles (UAVs and UGVs) and vehicles operating in urban environments.

1.1 Project description

Accurate and reliable localization of soldiers in all environments, including urban and indoor operations, is a challenge that has not yet been solved. Existing systems are not able to provide sufficient accuracy (approximately 3 meters) while simultaneously fulfilling the stringent size, weight and cost requirements.

GPS receivers can provide sufficient position accuracies in many environments. However, the GPS signals are very weak at the surface of the earth and they can easily be jammed. The GPS signal experiences reflection, scattering and attenuation in urban environments, and these effects may cause large position errors. Thus, the position accuracy and availability is often insufficient in urban environments, especially considering indoor operations.

By integrating the GPS receiver with additional positioning sensors, e.g. inertial sensors, magnetometers, barometric and/or imaging sensors, it is believed that the problem with providing an accurate soldier positioning system can be solved. Similar technologies can also be used in future positioning systems for small unmanned aerial/ground vehicles (UAVs/UGVs) and other vehicles operating in urban environments.

The project *Robust positioning for efficient C2* is a R&D project financed by the Swedish Armed Forces. The project started in 2011 and it ends in December 2013. The overall focus of the project has been to address research problems that are considered to be key areas for increasing the robustness and accuracy for military positioning systems. The aim is to demonstrate new technologies and possibilities for localizing soldiers and vehicles, with a particular emphasis on soldier positioning systems in urban environments.

1.2 Description of work

When performing sensor fusion it is crucial that accurate estimates of the errors in the different sensors/sub-systems are available. Hence, when integrated into a multisensor positioning system, it is important that unintentional interference, hostile jamming or spoofing can be detected before they affect the position accuracy of the GPS receiver.

The main goal of this work is to evaluate different approaches for detecting jamming signals in the GNSS frequency bands.

2 Current threats

The use of GNSS receivers is wide spread in the society today. GNSS receivers are used for navigation in many safety critical sectors, such as maritime, aviation and first responder applications, but also for timing synchronization in important infrastructural applications such as the power grid, mobile telephony systems and financial investment systems [1], [2]. With the wide spread usage and high reliance of GNSS, also comes vulnerability to outages due to interference, jamming and spoofing.

The vulnerabilities of GNSS were reported already over a decade ago in the Volpe report [3], and later in other publications (cf. [4]). Although GNSS jamming is illegal in most countries, there is a great range of commercial jammers available for less than a hundred dollars [5].

2.1 Examples of GPS jamming incidents

There are examples in the past few years when jammers have been used and affected GPS receivers, both purposely and accidentally [6], [7]. Examples of GPS jamming incidents:

- Biskopstorp, Oct. 18 2011 [8]: People reported that GPS and mobile phones did not work in an area in southern Sweden. The police investigated the problem and found stolen property, such as boat engines and car tires, worth over one million SEK. Jammers were used to prevent the stolen property from being tracked.
- Newark airport, Aug. 3 2012 [10]: Technicians had been experiencing interference during pre-deployment testing of a ground-based augmentation system (GBAS). It was found that a Ford F-150 pickup truck was emanating radio signals within the restricted 1559 to 1610 MHz band. The signals emanating from the vehicle were blocking the reception of GPS signals in the GBAS. The driver claimed that he installed and operated the jamming device in his company-supplied vehicle to block the GPS-based vehicle tracking system that his employer installed in the vehicle.
- Newark airport, New Jersey, 2009 [11]: Engineers noticed that GPS receivers at Newark airport were suffering brief daily breaks in reception. It took two months for investigators from the Federal Aviation Authority to track down the problem: a driver who passed by on the nearby highway each day had a cheap GPS jammer in his truck to prevent his employer from tracking the vehicle.
- San Diego, 2007 [12]: Two navy ships in the San Diego harbor conducted a training exercise. To test procedures when communications were lost, technicians jammed radio signals. Unwittingly, they also blocked radio signals from GPS satellites. A big part of central San Diego was affected. The system for tracking incoming planes at the airport was malfunctioning, emergency pagers used for summoning doctors at the Naval Medical Center stopped working, the traffic-management system used for guiding boats in the harbor failed, about 150 base stations were malfunctioning and cellphones did not work, and bank customers trying to withdraw cash from local ATMs were refused.
- North Korea [13]: GPS jamming has been performed in military exercises along the border on three documented occasions in March 2011, and in August and December of 2010. In addition, GPS jamming was performed in 2012 during April 28 and May 13. A large number of aircrafts and ships were affected.
- UK, July 2010 [14]: Two men were jailed for a total of 16 years after they admitted being members of a criminal gang that stole 40 trucks and their loads with a total value of £6 million. They had used GPS jammers to prevent the vehicles from being tracked after the thefts.

- Germany [14]: Truck drivers have used jammers to evade the country's GPS-based road-tolling system.

2.2 GPS jamming devices

There is a huge selection of commercial jammers available on the Internet for less than $100. What used to be expensive military technology a few decades ago are nowadays easily available, rather cheap, off-the-shelf products. Studies of many of these jammers have been performed, and they were categorized in [5] into the following three categories:

1. Jammers that are designed to plug into a 12 Volt car cigarette lighter socket power supply outlet. This category of jammers usually has rather low transmit power (below 100 mW) and the possibility to connect an external antenna. An example of a jammer from this category is shown in Figure 1.
2. Jammers that have an internal battery and an external antenna connected via an SMA connector. Some of these jammers transmit at both the L1 and L2 frequency bands, and additional frequency bands for other types of communication (e.g. WiFi and GSM). The transmit power is up to 1 W. An example of a jammer in this category is shown in Figure 2.
3. Jammers disguised as a harmless electronic device, such as a cell phone. The jammers in this group have internal batteries but no possibility to connect an external antenna. All jammers in this group that were tested in [5] transmit power in L1, L2 and additional frequency bands, with up to 100 mW power.

Figure 1. Commercial jammer from the first category of jammers.

Figure 2. RX-700 jammer, from the second category of jammers.

Most of the jammers that were studied in [5] transmitted signals with bandwidths exceeding the 2 MHz civilian C/A and L2C signals, and some had bandwidths even exceeding the 20 MHz military P(Y) signal. That is, most jammers are better adopted to jam the military GPS signal, and a big part of the transmit power is out-of-band for the civilian signal. Most of these jamming signals are generated by frequency modulation of a continuous wave (CW) signal with a saw-tooth or sine type of signal to achieve the desired bandwidth.

The current development of GPS jammers is extensive and even more advanced jammers than those in the three categories above start to show up. These jammers can transmit with powers above 1 W, and even up to 100 W. In addition to transmitting on multiple frequency bands these jammers can also make use of multiple antennas, but they are not necessarily handheld.

During the last few years, several research groups have shown in real field trials that it is possible to not only jam but spoof a GPS receiver in a controlled manner to change its perception of position and time [2], [15]. These trials were performed using relatively cheap equipment, and there is a high risk that similar equipment will be used for illicit purposes in the future.

2.3 GPS jamming towards military systems

GPS was developed as a military specific support system but today it is a *dual-use* system. GPS is used by the armed forces for a wide range of applications, ranging from soldier navigation to guidance of precision weapons. Position and timing information is crucial information in the command & control (C2) systems and in most cases this originates from either a military or a civil GPS-receiver. The use of military GPS is outlined in the NATO NAVWAR STANAG and CONOP, which states that the use shall be protected and maximized. Therefore it is important that the GPS receivers have a robust capability to detect jamming. Also, if jamming can be detected at a long distances, i.e. before the performance of the GPS-receiver is affected by jamming, the information can be used to give an indication of enemy activities both on tactical and on a strategic level.

For the ground forces position information is used by units and soldiers both to navigate and in C2-systems to achieve situational awareness. Based on the situational awareness picture it is possible to lead and use the forces more efficiently. New military weapon system such as Archer and Excalibur gives a precision strike capability. Excalibur is a precision artillery grenade with a GPS based navigation and guidance systems with high accuracy, CEP of 5 meters, and extremely long range, more than 50 km.

Most NATO air forces use military GPS receivers extensively, both for navigation and for air-to-ground precision strike capability. Several weapon systems have a military GPS receiver integrated as a complement to other sensors, for example the Enhanced Paveway

II. The JDAM (Joint Direct Attack Munitions) and SDBI (Small Diameter Bomb I) only uses GPS receivers to achieve the precision strike capability.

For maritime applications GPS is primarily used for navigation, in most cases integrated with INS. Timing information is used by several systems on a ship, for example communication, radar and electronic warfare systems. Modern ship-to-ship missiles with long range have an integrated military GPS-receiver.

There is a jamming threat against the military use of GPS both from so called internet jammers and military tactical jammers. Internet jammers can be a potential threat against military operations as they can be deployed by an enemy in an urban environment. Today on internet it's also possible to find GPS-jammers with high power and directional antennas that can be considered as a severe threat for several scenarios. Electronic warfare units have the capability to deploy jammers with kW output power and use directional antennas to increase the jamming range. A future threat will be from so called *emerging threat (ET) jammers* that can be combined with GPS jammers. Due to the extensive use of GPS in military applications the threat is expected to increase in the future.

3 Basics of detection theory

The first step to mitigate the effects of jamming is to detect the interfering signal and if the GNSS position and time solution is unreliable. The concept of detection theory is a well-studied topic since many decades, and there are several very good books on the topic (cf. [16], [17]). In the following, we will present some of the basics of detection theory that are needed for better understanding of the sequel of this chapter.

3.1 Hypothesis testing and the likelihood ratio

The problem of signal detection is to decide whether a signal is transmitted or not. That is, in its simplest form we want to discriminate between the two hypotheses

$$\begin{aligned} \boldsymbol{H_0}&: \boldsymbol{y}[\boldsymbol{n}] = \boldsymbol{e}[\boldsymbol{n}], \\ \boldsymbol{H_1}&: \boldsymbol{y}[\boldsymbol{n}] = \boldsymbol{x}[\boldsymbol{n}] + \boldsymbol{e}[\boldsymbol{n}], \end{aligned} \tag{1}$$

where $y[n]$ is the received signal, $x[n]$ represents the signal to be detected, $e[n]$ is noise plus interference (including signals which are not of interest to detect) and n represents time. Typically, a decision on one of the hypotheses is accomplished by first forming a test statistic $\Gamma(\boldsymbol{y})$ from the received data $\boldsymbol{y} \triangleq [y[1], y[2], \cdots y[N]]$, and then comparing $\Gamma(\boldsymbol{y})$ with a predetermined threshold η:

$$\boldsymbol{\Gamma(y)} \underset{\boldsymbol{H_0}}{\overset{\boldsymbol{H_1}}{\gtrless}} \boldsymbol{\eta}. \tag{2}$$

Clearly, the fundamental problem of detector design is to choose the test statistic $\Gamma(\boldsymbol{y})$ and to set the decision threshold η in order to achieve good detection performance.

3.2 Receiver operating characteristics (ROC)

The performance of a detector is quantified in terms of its *receiver operating characteristics* (ROC), which gives the probability of detection $P_D = \Pr(\Gamma(\boldsymbol{y}) > \eta | H_1)$ as a function of the probability of false alarm $P_{FA} = \Pr(\Gamma(\boldsymbol{y}) > \eta | H_0)$ at a certain SNR. By varying the decision threshold η, the operating point of a detector can be chosen anywhere along its ROC curve. There is always a tradeoff between detection probability and false-alarm probability. That is, increased detection probability always comes at the cost of increased false-alarm probability, and vice versa, decreased false-alarm probability comes at the cost of decreased detection probability. This tradeoff is exactly what is determined by the ROC.

3.3 Likelihood-ratio

Detection algorithms are either designed in the framework of classical statistics, or in the framework of Bayesian statistics. In the classical (also known as deterministic) framework, either H_0 or H_1 is deterministically true, and the objective is to choose $\Gamma(\boldsymbol{y})$ and η so as to maximize P_D subject to a constraint on P_{FA}: $P_{FA} \leq \alpha$. In the Bayesian framework, by contrast, it is assumed that the source selects the true hypothesis at random, according to some *a priori* probabilities $\Pr(H_0)$ and $\Pr(H_1)$. The objective in this framework is to minimize the so-called Bayesian cost. Interestingly, although the difference in philosophy between these two approaches is substantial, both result in a test of the form (2) where the test statistic is the likelihood-ratio [16]

$$\boldsymbol{\Gamma(y)} = \frac{\boldsymbol{p(y|H_1)}}{\boldsymbol{p(y|H_0)}}, \tag{3}$$

where $\boldsymbol{p(y|H_0)}$ and $\boldsymbol{p(y|H_1)}$ are the probability density functions of the received data $\boldsymbol{y}$ under hypothesis $\boldsymbol{H_0}$ and $\boldsymbol{H_1}$ respectively.

3.4 Energy detection

One of the simplest detection methods, used in many applications, is the energy detector, also known as the radiometer [18]. The energy detector measures the received signal energy during a finite time interval and compares it to a predefined decision threshold. That is, the test statistic of the energy detector is

$$\boldsymbol{\Gamma(y)} = \frac{\mathbf{1}}{\boldsymbol{N}}\sum_{\boldsymbol{n=1}}^{\boldsymbol{N}}|\boldsymbol{y[n]}|^{\mathbf{2}}, \tag{4}$$

where N is the number of samples. The energy detector is optimal (both in the Bayesian and Classical senses) for detection of a white Gaussian signal embedded in additive white Gaussian noise when the signal and noise powers $E\{|\boldsymbol{e[n]}|^{\mathbf{2}}\}$ and $E\{|\boldsymbol{x[n]}|^{\mathbf{2}}\}$, where $E\{\cdot\}$ denotes the expected value, are known. The energy detector can be used to detect any kinds of interference, and does not require any knowledge of the jamming signal to be detected. However, one drawback with the energy detector in practice is the problem of determining the decision threshold appropriately, since the noise (plus interference) power is never perfectly known. In practice, one is forced to collect data that is not affected by a jamming signal and either estimate the noise power or, more commonly, set the threshold based directly on the test statistics from the jamming free data based on a predetermined false-alarm rate. An alternative could also be to set the decision threshold to achieve a predetermined detection rate based on a set of jammed data. However, the threshold will then depend on the jammer signal power and the characteristics of the signal, and this approach is therefore usually not a feasible solution.

3.5 Model uncertainties, SNR wall and CFAR detection

To compute the likelihood ratio (3**)**, the probability distribution of the observation $\boldsymbol{y}$ must be perfectly known under both hypotheses (i.e. that the signal is present or not). This means that one must know all parameters, such as noise and signal powers. In any case, the signal and noise in (1) must be modeled with some known distributions. Of course, a model is always a simplification of reality, and the true probability distributions are never perfectly known. Even if the model would be perfectly consistent with reality, there will always be some parameters that are imperfectly known such as the noise and signal powers as noted above. For example, the performance of the energy detector is well known to degrade significantly if the noise power estimate is erroneous, even when the noise and signal are perfectly Gaussian. In practice, a jammer signal is often not even close to Gaussian, which would potentially degrade the detection performance further. It should be noted, however, that the energy detector can detect all kinds of signals that increase the average power even though neither the noise nor the signal are Gaussian, but it is generally not the optimal detector.

Even if a valid test statistic is designed based on some other properties, without considering the likelihoods, the decision threshold must be set appropriately. In many cases, at least the noise (plus interference) power has to be known to set the threshold. However, a detector is said to have the property of constant-false alarm rate (CFAR) if its false alarm probability is kept constant and therefore is independent of any unknown parameters. In particular, the CFAR property means that the decision threshold is independent of the noise power, and therefore can be set to achieve a pre-specified value without knowing the level of the noise power. A necessary condition for the CFAR property is that the test statistic is dimensionless, and therefore the problem is invariant to

a scaling of the unknown parameters. The CFAR property implies, for example, that the test statistic is unaffected by a varying noise power. This also implies that if the decision threshold is set empirically based on a set of noise-only data as explained before, the threshold is also unaffected by a varying noise power during the measurement.

Perhaps more importantly, there are fundamental limits on detection at low signal-to-noise ratio (SNR). The SNR is defined as $E\{|\boldsymbol{x}[\boldsymbol{n}]|^2\}/E\{|\boldsymbol{e}[\boldsymbol{n}]|^2\}$. Specifically, due to uncertainties in the model assumptions, accurate detection is impossible below a certain SNR level, known as the *SNR wall* [19] [20]. The problem with noise power uncertainty for the energy detector is just one example of this. Other model uncertainties that could affect the detection performance are, for example, imperfect knowledge or idealized system model assumptions of the channel, time and frequency synchronization, I/Q imbalance, and A/D conversion. Luckily, it is possible to mitigate the problem of SNR walls, by taking these imperfections into account, in the sense that the SNR wall can be moved to a lower SNR level.

4 GNSS jamming detection – a literature survey

Numerous interference and jamming detectors for GNSS receivers have been proposed during the last few years, based on various properties of the received signal. A brief survey of the previous work on GNSS jamming detection will be given in the following sections.

4.1 Energy detectors

The simplest and most commonly used detection method is the energy detector, as presented in Section3.4. Variations of the standard energy detector can be performed in the time domain as well as in the frequency domain.

A frequency domain detector was proposed in [21] for detection of a narrowband continuous wave (CW) interference signal being captured by a GPS receiver. The spectral components were estimated using an averaged fast Fourier transform (FFT). The noise parameters (mean and variance of the power) were assumed in [21] to be estimated from an assessment window which is not subject to interference, in order to set a decision threshold to achieve a predetermined false-alarm probability. The actual test statistic of [21] is based on the difference of the estimated mean values obtained from the assessment window and the evaluation window respectively, normalized by the estimated variances. The same approach was also taken in [22], but the spectral components were estimated using a windowed (Welch) periodogram, rather than the standard periodogram calculated with the FFT.

Several measures are proposed in [23] that could be used for interference detection. The proposed test statistics are estimates of correlator output power (normalized by estimated receiver noise), standard deviation of correlator output power, carrier phase vacillation and automatic gain control (AGC) level. These measures are motivated in [23] by the correlation between the position error and each measure, which is obtained from test bench measurements. Automatic gain control is used to control the dynamic range of the input signal to the receiver amplifier. In essence, an AGC measures the average value of the input signal and adjusts the amplifier gain so as to keep the output signal constant. Jamming detection based on the AGC level in a GPS receiver was also proposed and analyzed in [24].

A detector based on the AGC level is very similar to an energy detector, and therefore also inherits its pros and cons. The main advantage of using an AGC based detector rather than an energy detector is that the AGC data can be available from a standard commercial GNSS receiver, whereas the raw IF data that is required to compute the energy is generally not. Some of the drawbacks of the AGC detector, compared to an energy detector, are that the AGC levels are quantized and there is no flexibility to set the detection time as desired (determined by the hardware used in the measurement).

The main advantage of the detectors in this section is that they can be used to detect any type of signal, and does not require any knowledge of the signal to be detected. A common problem with these detectors, however, is how to set the decision threshold properly since they are not CFAR detectors.

4.2 C/N_0-based detectors

The carrier-to-noise (C/N_0) ratio, i.e. the ratio of the useful power of a certain GNSS satellite signal to the noise power, is a measurement of the received signal quality from the corresponding satellite. Estimates of the C/N_0 are provided by commercial GNSS receivers and can be used for detection without requiring access to the internal signal processing in the GNSS chipset. This was done for example in [25] by approximating the

C/N_0 estimate for each satellite signal as Gaussian, to obtain the decision threshold. Thus, one jamming detector for each satellite signal is effectively used. Estimates of individual satellite C/N_0 were also used in [26] to characterize and detect a continuous wave (CW) interference signal. The paper [27] considered both pre- and post-correlation detection methods, through energy detection and C/N_0 estimation respectively. The work of [27] was done within the EU FP7 project DETECTOR. One major drawback with C/N_0-based detectors is that these estimates cannot distinguish between an increased noise-plus-jammer-power and a decreased desired signal power, since the C/N_0 estimates decrease both when the GPS receiver is jammed and when the desired GPS signal is attenuated by buildings or other objects, which commonly occur in urban areas.

The main advantage of the C/N_0-based detectors is, just like the energy based detectors, that they can be used to detect any type of interference signal. However, a serious disadvantage of these detectors is that they cannot distinguish between decreased GNSS signal powers and increased interference power. Therefore, this type of detectors is only useful in situations where the GNSS signal strength is normally fairly constant. For example, these detectors could be used at fixed positions along roadsides or at critical infrastructure, but are not suitable in mobile scenarios in urban environments where the satellite signal strength varies because of attenuation caused by the surrounding buildings.

4.3 Detectors based on correlation with other sensors

If a GNSS receiver is integrated with other sensors, detection can be performed by exploiting the combined information from all sensors. Interference detection based on a combination of GNSS and an inertial navigation system (INS) was considered in [28]. The detector of [28] is based on changes of the covariance estimate from the extended Kalman filter. The papers [29] and [30] propose a spoofing and interference detector that uses a secure reference receiver to correlate the encrypted and unknown P(Y) signals at the two receivers. This detector relies on the presence of the military P(Y) signal on the same frequency and with a known relationship of timing and carrier phase with the publicly known C/A signal. The intuition behind the detector of [29], [30] is that the correlation with the signal received at the reference receiver will decrease if the receiver is being spoofed or interfered. Clearly, if information from multiple sensors is available, it should be beneficial to exploit this information for detection. The detectors could potentially become quite complex, both in terms of the development of good detectors and in terms of real-time computational complexity.

4.4 Detection with antenna arrays

Multiple antennas can be used to detect an interfering signal by exploiting the spatial properties of signals received from satellites and from a jammer respectively (i.e. they arrive from different directions). Such a detector was, for example, proposed in [31], where the phase difference between two receive antennas was estimated and used to detect a spoofing signal. A spoofing detector that exploits the spatial correlation of the signal received from a spoofer with a single antenna was also proposed in [32] and [33]. The spatial correlation is obtained through a single receive antenna in movement, which thereby comprises a synthetic antenna array by collecting samples at different positions. The detector is then based on estimates of the correlation coefficients of the data after despreading. Another detector that exploits the spatial properties of a single moving antenna, through the carrier phase correlation, was proposed in [34] and [35]. The detector of [34] and [35] requires, and exploits, knowledge of the antenna movement, whereas the detector of [32] and [33] does not. The spatial correlation of the received signal should be inherent also for any other type of jamming signal even before the despreading. It should also be noted that the same spatial properties will be inherent if the signal is received by

multiple antennas separated sufficiently far away from each other. Analogously, other multiple antenna detectors that exploit the spatial correlation could be applied in a similar manner on a synthetic antenna array. Many other multiple antenna detectors exist in the literature, although in many cases originally intended for other applications (cf. [36] and the references therein). Multiple antenna methods can be used to achieve CFAR detection (cf. [36]). In addition, antenna arrays can be used not only to detect the jammer, but also to mitigate the effect of interference by beamforming and nulling techniques. An obvious drawback of these methods is that it may be practically infeasible to have an antenna array on the platform, and the cost is higher.

4.5 Detection and mitigation based on various measurements

Various other measure, than those described above could also be exploited for detection of interference and jamming. The following methods were also mentioned in [31] as potential ways of discriminating a spoofing signal from an authentic GNSS signal;

- amplitude discrimination,
- time-of-arrival discrimination,
- cross check with other navigation sensors such as an inertial measurement unit (IMU),
- polarization discrimination,
- angle-of-arrival discrimination,
- cryptographic authentication.

Signal properties that are exploited for detection can also be exploited to mitigate the effects of interference and jamming. Mitigation techniques were mentioned in [37], based on

- adaptive notch filtering,
- frequency switching,
- combining GNSS with other navigation sensors such as an IMU,
- multiple antenna techniques such as beamforming and nulling.

Different techniques are suitable for different types of interfering signals. Notch filtering, for example, is suitable to filter out a narrow band CW signal but not for a wide band signal.

5 Test results

In this study, we have evaluated the performance of a few rather simple detectors. The focus has been to investigate the performance of detection of unknown jammer signals. Therefore, all feature detectors that exploit specific signal properties have been excluded. Only detectors that exploit the general signal property of increased received signal power have been studied. The study includes standard energy detection, AGC-based detection and C/N_0–based detection.

The following sections show evaluations of standard energy detection, AGC-based detection and C/N_0–based detection. The evaluation of the energy detector is based on measurements of raw IF data in the lab, whereas the evaluations of AGC detection and C/N_0–based detection are based on outdoor field trials. The setups for these tests will be described in more detail in the following sections.

5.1 Energy detection

Raw IF data has been collected in the lab using a Universal Software Radio Peripheral (USRP) [38], which is a software radio platform, and an RX-700 jammer, which is a commercial GPS jammer, connected via cable. The Rx-700 jammer transmits a very wide band (> 50 MHz) signal in the L1 frequency band, as shown in Figure 3. The USRP that was used in the measurements was an N200 [39] with a WBX 50-2200 MHz Rx/Tx daughterboard [40]. Attenuators were used between the jammer and the receiver to collect data at different jammer-to-noise ratios (J/N). Data has also been collected with a 50 ohm termination on the antenna input, and the jammer disconnected (and turned off), to obtain noise-only data. Two minutes of complex data was stored for each case, using a sampling frequency of 3.846153 MHz with the frequency band centered on the L1 center frequency (1575.42 MHz).

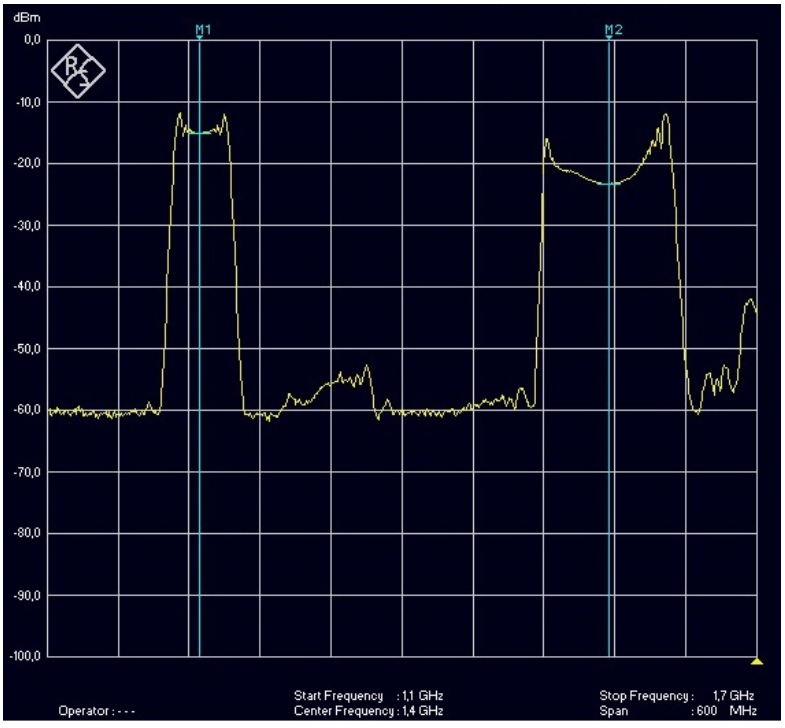

Figure 3. Spectrum of the RX-700 jammer. The vertical bluish lines show the GPS L1 and L2 center frequencies respectively.

It should be noted that these measurements have been performed indoors without any antenna, so that no satellite signals are actually being received. In practice, the GPS signals will increase the received power also during the noise measurements, so that the decision threshold must be adopted accordingly. In particular, the variations of the total received satellite signal power and its effect on the decision threshold and consequently the detection performance, need to be further analyzed and tested in real scenarios. In addition to signal power variations due to the authentic GPS signals, there are other potential interference sources, such as intersystem interference generated by e.g electronic equipment (laptops for example), that has to be considered. Whether unintentional interference sources should affect the decision threshold or not, depends of course whether these sources are to be detected or not. If the task is to detect intentional jammers only, the effect from unintentional interference on the decision threshold is probably larger than the effect caused by the authentic GPS signals.

Attenuators with 20, 23, 26 and 29 dB attenuation respectively were used between the jammer and the receiver in order to vary the received J/N in a controlled manner. The received J/N for each attenuator was estimated (in linear scale) as

$$\frac{\boldsymbol{J}}{\boldsymbol{N}} = \frac{\widehat{\boldsymbol{J}+\boldsymbol{N}} - \widehat{\boldsymbol{N}}}{\widehat{\boldsymbol{N}}}, \tag{5}$$

where $\widehat{\boldsymbol{N}}$ is the average power for the measurement with a 50 ohm termination, and $\widehat{\boldsymbol{J}+\boldsymbol{N}}$ is the average power for each measurement when using the corresponding attenuator of interest. The estimated J/N values are shown in Table 1. The estimator (5) assumes that the noise power (i.e. all power except the jammer signal) is constant during the noise measurement (50 ohm termination) and the jammer measurements. Ideally, the J/N difference between the levels should be 3 dB since the jammer signal is attenuated in steps of 3 dB. However, the estimated J/N values shown in Table 1 indicate that the background noise power during the jammer measurements is slightly higher, since the difference of the estimated J/N between the levels decreases with increasing attenuation. The reason for this is not all clear, but it could be caused by leakage from the jammer.

Table 1. Estimated J/N for the corresponding jamming signal attenuations.

Attenuation [dB]	**20**	**23**	**26**	**29**
Estimated J/N [dB]	-3,1	-7,8	-10,8	-11,8

Detection performance is completely determined by the probability density function (PDF) of the test statistic under the two hypotheses. The estimated PDF of the test statistic of an energy detector with a detection time of 10^{-4} seconds, corresponding to roughly 384 samples, for the two hypotheses is shown in Figure 4 for two different J/N values. The detection performance is of course better at a higher J/N, which is also seen by the larger difference of the PDFs under the two hypotheses in the leftmost plot as compared to the rightmost plot.

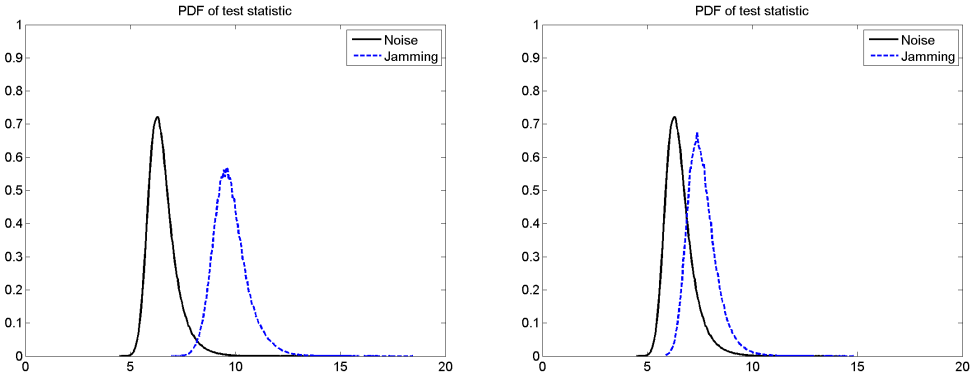

Figure 4. Estimated PDF of the test statistic, for a detection time of 10^{-4} seconds, under the two hypotheses (noise only and jamming plus noise) at different J/N levels.

Figure 5 shows the ROC curves for the energy detector with a detection time of 10^{-4} seconds, using the 20, 23, 26 and 29 dB attenuators between the jammer and receiver respectively as described above. Clearly, at a higher J/N (lower attenuation) the detector achieves higher detection rate for the same false-alarm rate than at lower J/N. It is also seen in the figure that the performance difference between the curves decreases with increasing J/N, which is consistent with the estimated J/N as shown in Table 1. That is, the difference between the red 26 dB curve and the green 29 dB curve is smaller than the difference between the black 20 dB and blue 23 dB curves, which is in accordance with the differences of the estimated J/N (approximately 1 and 5 dB for the two cases respectively). For a given J/N, the operating point of the detector, corresponding to a specific pair of detection and false-alarm probabilities or equivalently a decision threshold, can be chosen anywhere along the corresponding ROC curve. This also shows the tradeoff between the detection and false-alarm probabilities. The consequence of not setting the decision threshold appropriately, as discussed in Section 3.5, is that the actual operating point is not equal to the desired operating point.

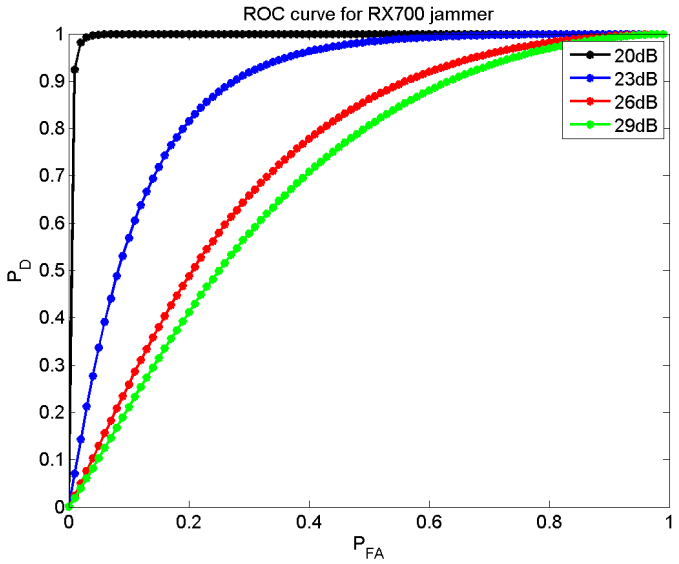

Figure 5. ROC curves, for a detection time of 10^{-4} seconds, at different J/N levels (expressed as the attenuation of the jamming signal).

Figure 6 shows the detection probability as a function of the estimated J/N. The left figure shows the results for different detection times (10^{-3}, 10^{-4} and 10^{-5} seconds) and $P_{FA} = 0.01$. It is clear that a higher detection probability is achieved with a longer detection time. Intuitively, doubling the detection time should be approximately equivalent to doubling (increasing with 3 dB) the J/N. For white Gaussian signal and noise, this relation is exact. In the left plot of Figure 6, the difference between the curves is not 10 dB although the detection time differs with an order of magnitude. The reasons are that the J/N estimate is imperfect as explained above, and that both the jammer signal and the noise are non-Gaussian. Of course, the performance gain from using a longer detection time, comes at the cost of a slower detection. The right figure shows the results for different false-alarm probabilities (0.1, 0.01 and 0.001) and a detection time of 10^{-4} seconds. Again, it is seen that a higher detection probability can be achieved if a higher false-alarm probability is allowed.

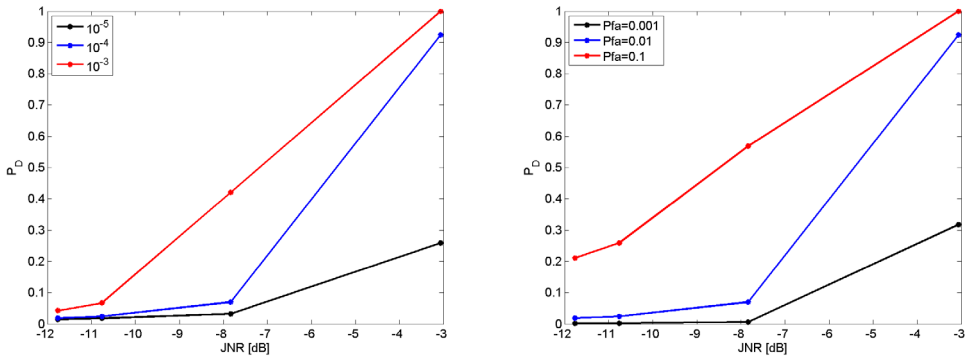

Figure 6. Probability of detection as a function of estimated J/N, for detection times 10^{-3}, 10^{-4} and 10^{-5} seconds (left) and varying false-alarm probability (right).

The results of this section essentially show the detection performance of using a standard energy detector on a USRP. The performance of this detector in more realistic scenarios needs to be further analyzed, in order to draw any strong conclusions. As shown, the actual performance of the detector depends very much on the desired operating point (false-alarm and detection probabilities) including the ability to set the decision threshold and the detection time appropriately. These are parameters that can be chosen arbitrarily, depending on the application requirements. For example, the jammer is detected almost certainly at -3 dB J/N when using a 10^{-3} seconds detection time and 0.01 probability of false-alarm, or a 10^{-4} seconds detection time and 0.1 probability of false-alarm. To guarantee almost certain detection at lower J/N, one has to increase the detection time or allow a larger amount of false-alarms.

5.2 AGC detection

Parts of the results in this section were published in [41]. The detectors in this test are based on the AGC level, and two different receivers have been tested; a Novatel and a USRP. The Novatel GPS receiver provides its AGC information over a proprietary message which gives details about the internal ADC and amplifier. Past experience has shown this to be quite sensitive and an effective measure of in-band power [24]. Shown for this work is a dimensionless metric of the amplifier gain. Raw IF samples were collected during the experiment with a USRP. The resulting IF data stream was used to estimate in-band power which was translated to a comparable AGC metric. The decision thresholds have been set in a similar manner as explained before, to achieve a predetermined false-alarm rate based on noise-only measurements.

The jamming signals that were used in the trials in this section were

- a continuous wave (CW) at 1575.42 MHz (L1 center frequency),
- a frequency modulated CW (MCW) swept at 1 Hz, ±150 kHz around 1575.42 MHz,
- a BPSK modulated signal with approximately 2 MHz bandwidth,
- a BPSK modulated signal with approximately 20 MHz bandwidth.

In this test, the jammer and the GPS receiver were placed in fixed positions, and the jammer signal power was varied in a controlled manner so that the detection performance can be evaluated and compared at different jammer-to-signal ratios (J/S). The J/S has been estimated based on the output power, antenna gains, measured cable losses, and path loss based on the distance between the jammer and the receivers. During this trial, the jammer transmit power was increased in steps of 2 dB over a range of 30 dB, with 30 seconds at each power level.

The recorded AGC levels and estimated J/S from these measurements, and the decision thresholds for false-alarm rates of 0.05, 0.01 and 0.001 respectively, are shown in Figure 7-Figure 10 for the different types of jammer signals. Since the AGC values decreases with increasing received signal strength, a jammer is detected when the AGC level is below the threshold. Consequently, the decision threshold is lower, so that the jammer signal is detected at a higher J/S, for a smaller false-alarm probability. The left plots show the results for the Novatel receiver and the right plots show the results for the USRP. Due to problems with the data storage, some data is missing in Figure 7 for the USRP and in Figure 10 for the jammer power. However, the most interesting parts of the test are still visible since the data is missing at the end of the corresponding tests only.

The detection performance for both receivers is roughly the same for all kinds of signals that were tested. All signals are detected at a J/S of roughly 19-29 dB for the USRP and 41-47 dB for the Novatel, depending on the decision threshold and type of signal. The differences between the two receivers depend mainly on the hardware and on the implementations of the AGC. Based on the limited amount of data, it is hard to say if the small performance differences from the different measurements depend on the actual signal type or on differences in the radio environment during the tests. The available data to set the decision threshold was unfortunately rather limited from these tests, which is the main reason that there is only a very small difference between some of the decision thresholds at different false-alarm rates. In particular, the decision thresholds for the Novatel for $P_{FA} = 0.1$ and $P_{FA} = 0.001$ are hard to distinguish from one another in the figures. In addition, the ‘noise-only’ data that is used to set the threshold is probably contaminated with a weak jammer signal, because the jammer was turned on but attenuated with a high attenuation. As a consequence, the performance of these detectors as shown in this section could be improved by adjusting the threshold based on truly interference-free data.

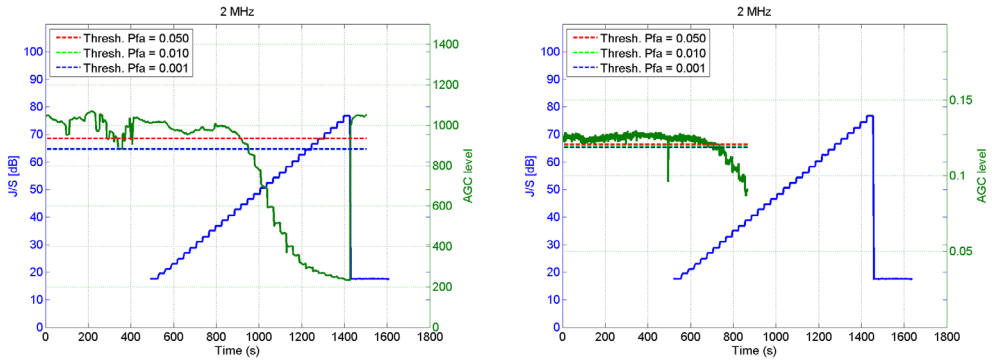

Figure 7. AGC levels, J/S for the 2 MHz signal and decision thresholds for the pre-specified false-alarm rates, for the Novatel (left) and the USRP (right).

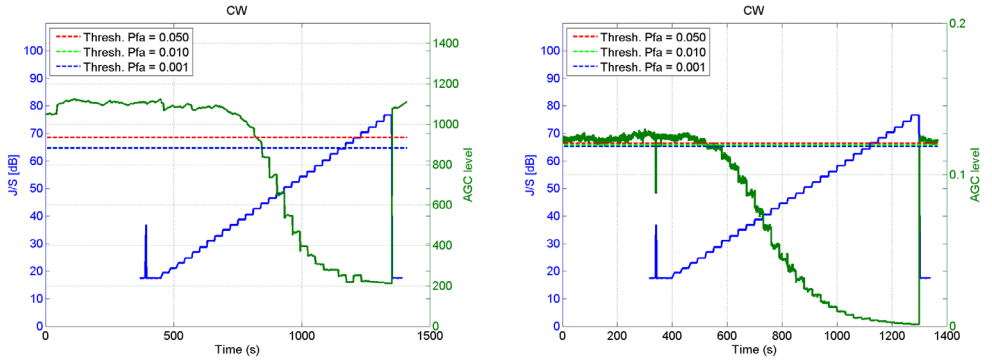

Figure 8. AGC levels, J/S for the CW signal and decision thresholds for the pre-specified false-alarm rates, for the Novatel (left) and the USRP (right).

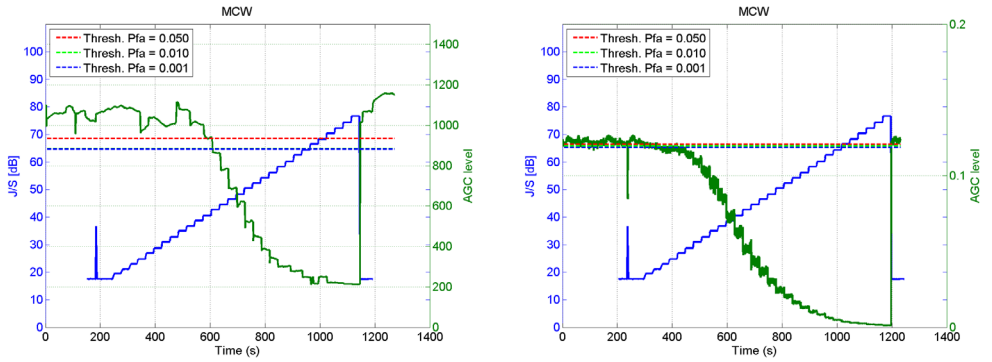

Figure 9. AGC levels, J/S for the MCW signal and decision thresholds for the prespecified false-alarm rates, for the Novatel (left) and the USRP (right).

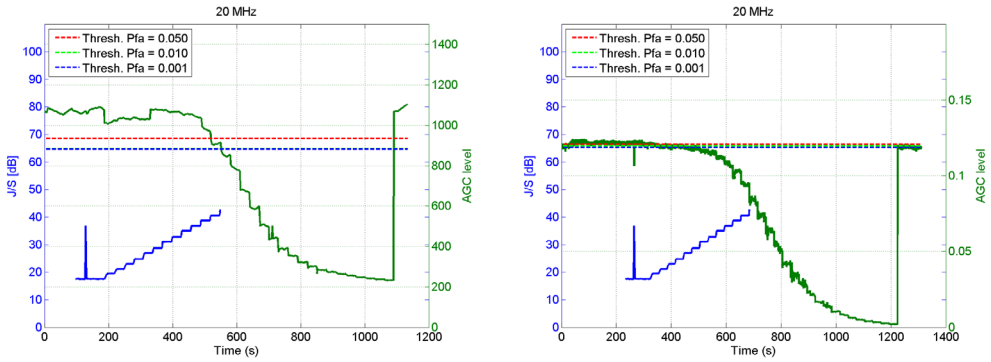

Figure 10. AGC levels, J/S for the 20 MHz signal and decision thresholds for the prespecified false-alarm rates, for the Novatel (left) and the USRP (right).

Figure 11-Figure 14 show the detection rate as a function of J/S for the two detectors, and for the same types of jammer signals as before. The J/S that is shown in the figures is the average of the estimated J/S during the 30 seconds of each power level.

It is clear from these figures that the USRP outperforms the Novatel with roughly 15-20 dB J/S for all types of signals. It can also be seen that an order of magnitude change in the false-alarm rate, at these false-alarm levels, changes the detection performance in the order of one dB J/S for both receivers. Again, it is hard to say if the small performance differences between the tests depend on the type of signal or other uncontrolled differences during the tests. It should be noted that, in theory, the detection probability should approach the desired false-alarm rate at low J/S. That is not observed in the figures, but the detection rate seems to approach zero. This is an artifact of the limited amount of data to obtain reliable statistics and that the decision threshold is not determined based on truly interference-free data. In addition, the Novatel gives an AGC value only once every second, whereas the USRP gives a value 55 times every second. That is, USRP detection is more reliable and faster than the Novatel. The reason for the performance difference between the USRP and the Novatel is not all clear. Although the Novatel outputs an AGC value once every second, this value does probably not correspond to a detection time (collection of data) of one second. The difference can also depend partially on the different hardware, in particular the receiver sensitivity. However, this has not been confirmed and it is a bit unexpected since, on the one hand the Novatel receiver is a couple of years old, but on the other hand the USRP is a quite simple and cheap low-end receiver.

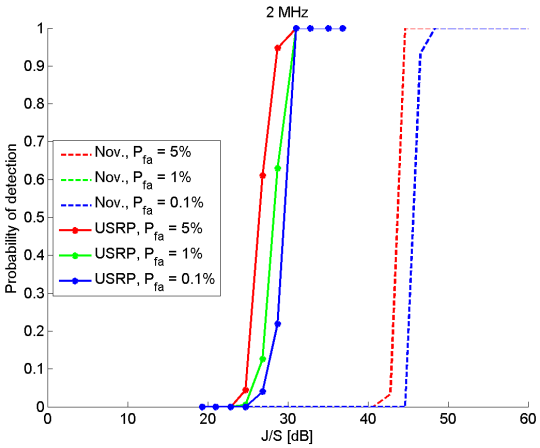

Figure 11. Probability of detection as a function of J/S for the 2 MHz signal, for the Novatel (dashed line) and the USRP (solid line) respectively.

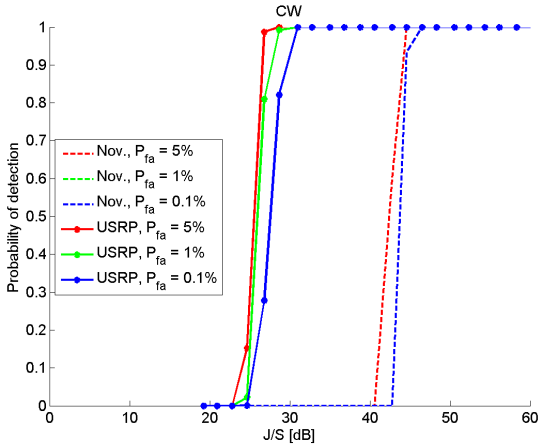

Figure 12. Probability of detection as a function of J/S for the CW signal, for the Novatel (dashed line) and the USRP (solid line) respectively.

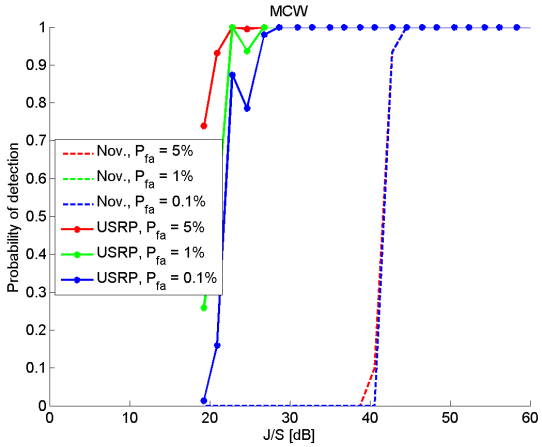

Figure 13. Probability of detection as a function of J/S for the MCW signal, for the Novatel (dashed line) and the USRP (solid line) respectively.

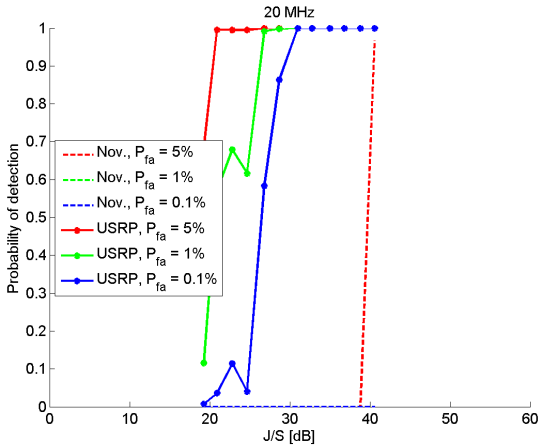

Figure 14. Probability of detection as a function of J/S for the 20 MHz signal, for the Novatel (dashed line) and the USRP (solid line) respectively.

5.3 C/N_0–based detection

Parts of the results, related to the Android application, in this section were published in [41]. The setup for this test is similar to the one in Section 5.2, so that the jammer and the GPS receiver were placed in fixed positions, and the jammer transmit power was changed in steps of 2 dB over a range of 30 dB, with 30 seconds at each power level. At the beginning and at the end of the test, the jammer transmit power was set at the maximum level. The only reason for this was to simplify the synchronization of data for the analyses, and it should not affect the results.

C/N_0-based detection was tested on two receivers, a Ublox 6H receiver and an Android application on a Sony Ericsson phone. The Android application gives a binary decision when the situation is alright, or there is a potential jamming signal. When no satellites are tracked, no decision is given at all. The detector application is based on the C/N_0 estimate as reported from the GPS receiver, which is available through the Android interface. The average C/N_0 of the used satellites is used as a test statistic for the Ublox receiver, and the decision thresholds have been set to achieve a predetermined false-alarm probability based on non-interfered measurements of the average C/N_0. The average C/N_0 from the non-interfered measurement, together with the decision thresholds are shown in Figure 15. Just as for the AGC levels, the decision threshold is lower at a lower false-alarm probability, since the average C/N_0 decreases with increasing jammer power. Hence, the fraction of values that lies below each decision threshold in Figure 15 is equal to the desired false-alarm probability for the corresponding threshold.

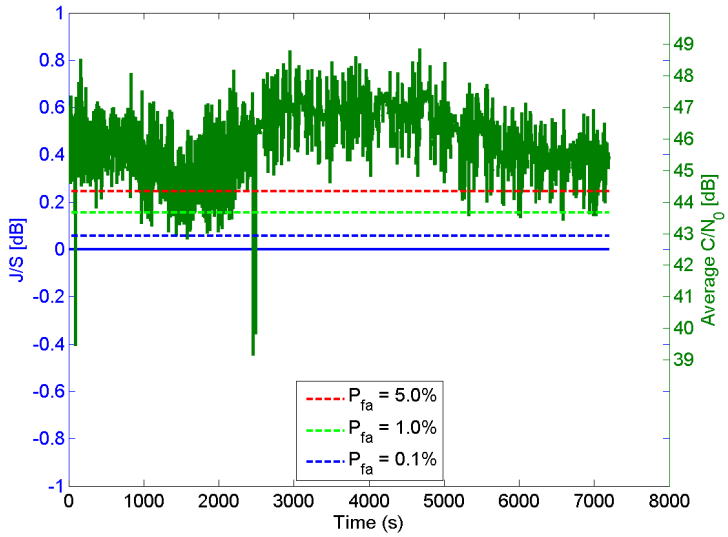

Figure 15. Average C/N0, and decision thresholds, for a non-interfered measurement with a Ublox receiver.

The average of the estimated C/N_0 and the estimated J/S from these measurements are shown in Figure 16-Figure 18. The figures also show the decision thresholds for false-alarm rates of 0.05, 0.01 and 0.001 respectively for the Ublox receiver (left figures), and the decisions (Jam Indicator) for the Android application (right figures). It can be seen in Figure 16 that the average C/N_0 decreases immediately when the jammer is turned on at the lowest power level at time 0. That is, the GPS receiver is actually affected, in the sense that the received satellite signal quality is lowered, during these tests even at the lowest power level.

Figure 16-Figure 18 show that all of these jammer signals can be detected by these methods in this scenario. The performance of the Android application is similar for all types of signals. The performance of the Ublox receiver is similar for the MCW and the 20 MHz signal, but the 2 MHz signal is detected already at the lowest tested power level

(J/S≈29 dB). For all types of signals, the Ublox detects the jammer signal at approximately 5-20 dB lower J/S than the Android application, depending on the decision threshold and the type of signal. However, since we do not have the possibility to set the decision threshold, or even know how it is set, for the Android application it is hard to make a fair comparison of the two receivers. The difference in performance is, however, not only due to the decision threshold but also due to differences in the receiver hardware and antennas. For example, the Ublox receiver was connected to an external antenna whereas the cell phone has its own built-in antenna, which is probably not as good as the external antenna.

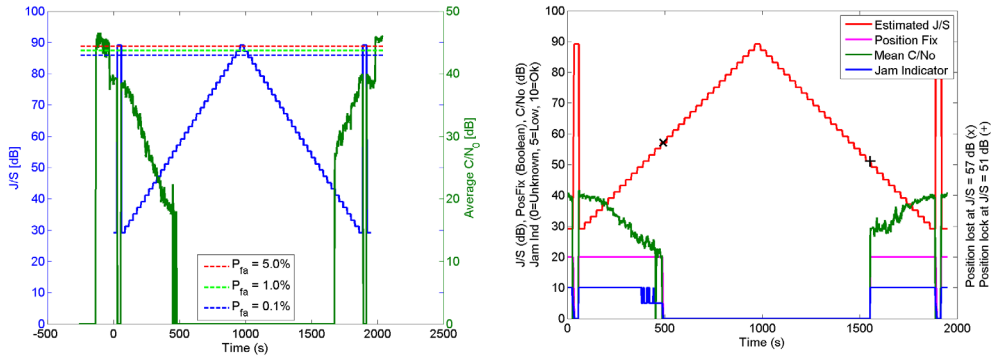

Figure 16. C/N_0-based detection of 2 MHz signal with a Ublox (left) and an Android application (right).

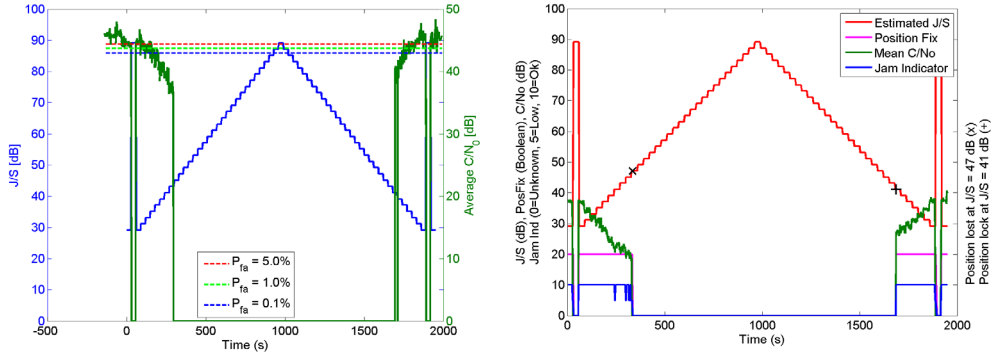

Figure 17. C/N_0-based detection of MCW signal with a Ublox (left) and an Android application (right).

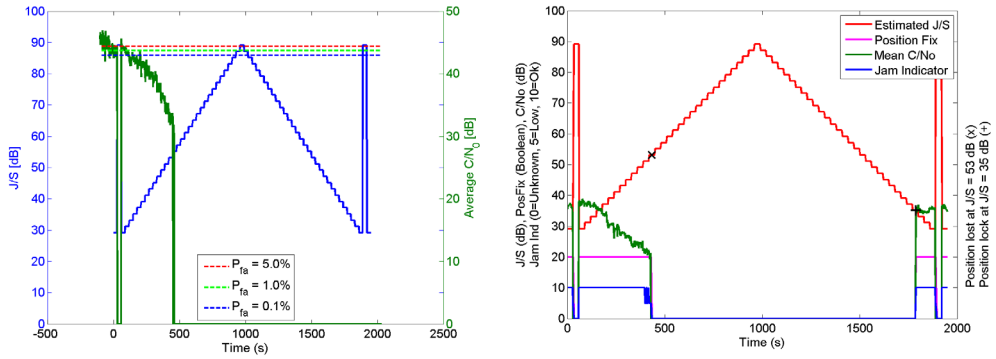

Figure 18. C/N_0-based detection of 20 MHz signal with a Ublox (left) and an Android application (right).

It should be noted that C/N_0-based detectors could work well in a static scenario, for example along roadsides, but are not suitable in a dynamic urban scenario, since they cannot distinguish between decreased GPS signal strength (e.g. indoors) and an increased interference level. This was also confirmed in a test that is reported in [41]. It is also worth noting that although essentially all types of jamming signals can be detected based on the C/N_0 estimates, a spoofing signal cannot. The reason is simply that the receiver will track the spoofing signal instead of the authentic signal, and the C/N_0 will probably not decrease.

6 Conclusions

This report has presented a survey of the basics of detection theory and previous work on GNSS jamming detection. A few simple, yet effective, detection methods have been evaluated based on measurements of real GPS and jamming signals. The main goal of the work has been to evaluate the ability to detect any kind of jammer signal. Therefore the focus of the evaluation has been on detectors that makes no assumption on the signal type of the jammer. It has been shown that detectors based on received energy, automatic gain control (AGC) levels, and receiver C/N_0 estimates are able to detect many different types of signals ranging from very narrow band (continuous wave) signals to very wide band (>20 MHz) signals. A problem with all of these detectors is to set the decision threshold properly, in order to detect harmful signals with good reliability but at the same time not give a large number of false alarms.

The performance of the different methods depends very much on the application and its requirements, as well as on the hardware and the possibility to change parameters such as the decision threshold and detection time.

Energy detection is a very simple, and often close to optimal (cf. [36] and the references therein), detector. However, to compute the energy, one essentially needs to have access to the raw IF samples. These are generally not available in an off-the-shelf product. AGC values could be available and therefore an AGC based detector could be a good alternative to the energy detector, with similar properties. Of course, the AGC gain is necessarily quantized, and as such some detection performance is lost as compared to dealing with raw IF data.

C/N_0–based detectors in general are not suitable for applications where the received satellite signal strength normally varies, such as dynamic scenarios in urban environments. This is due to that these detectors cannot distinguish between an increased noise-plus-jammer-power and a decreased GNSS signal power. Moreover, this type of detectors cannot detect jamming signalswhen the receiver has completely lost track of the satellites. That is, if the jamming signal power is too high it will not be detected at all. For energy and AGC based (and most other) detectors, the jammer signal is of course easier to detect the higher the power is.

6.1 Suggestions for future work

The energy detector and the AGC detector theoretically should work also for detection of a spoofing or ET jammer type of signal, since the total signal power is inevitably increased by a spoofer. However, C/N_0–based detectors are not able to detect a spoofing signal, since the C/N_0 would rather increase than decrease in the presence of a spoofer. Spoofing an ET jamming detection with energy and AGC detectors should be further tested and analyzed.

The natural variations of the received power and C/N_0 should also be further investigated. It is not clear how these natural variations in non-jammed environments affect the levels of the test statistics, and consequently how the decision thresholds should be determined. This is of particular interest in urban environments where the interference levels are higher and also are spatially correlated.

Impulse jamming signals were not considered in this work. Interference signals that are highly impulsive could have a significantly different impact on a GNSS receiver and on the detection performance than the non-impulsive signals that were tested in this work. The effect of impulse interference should be further investigated, both in terms of receiver impact and detection performance.

7 References

[1] D. P. Shepard, T. E. Humphreys and A. A. Fansler, "Going Up Against Time - The Power Grid's Vulnerability to GPS Spoofing Attacks," *GPS World,* pp. 34-38, Aug 2012.

[2] K. Wesson, D. P. Shepard and T. E. Humphreys, "Straight Talk on Anti-Spoofing -- Securing the Future of PNT," *GPS World,* pp. 32-34, 59-63, Jan 2012.

[3] J. A. Volpe, "Vulnerability Assessment of the Transportation Infrastructure Relying on the Global Positioning System," National Transportation Systems Center, 2001.

[4] D. Hoey and P. Benshoof , "Civil GPS Systems and Potential Vulnerabilities," in *ION GNSS*, Long Beach, California, 2005.

[5] R. H. Mitch, R. C. Dougherty, M. L. Psiaki, S. P. Powell, B. W. O'Hanlon, J. A. Bhatti and T. E. Humphreys, "Know Your Enemy - Signal Characteristics of Civil GPS Jammers," *GPS World,* vol. 23, no. 1, pp. 64-71, Jan 2012.

[6] S. Pullen and G. X. Gao, "GNSS Jamming in the Name of Privacy - Potential Threat to GPS Aviation," *Inside GNSS,* vol. 7, no. 2, pp. 34-43, Mar-Apr 2012.

[7] L. Scott, "Spoofs, Proofs & Jamming: Towards a Sound National Policy for Civil Location and Time Assurance," *InsideGNSS,* vol. 7, no. 5, pp. 42-53, October 2012.

[8] "Störningssändare skulle skydda stöldgods," *Hallandsposten,* 4 Jan 2012.

[9] "Två av tre fälls i hälerihärvan," *Hallandsposten,* 22 Feb 2012.

[10] Federal Communications Commission, *NOTICE OF APPARENT LIABILITY FOR FORFEITURE, FCC 13-106,* 2013.

[11] J. Warburton and C. Tedeschi, "GPS Privacy Jammers and RFI at Newark: Navigation Team AJP-652 Results," Federal Aviation Administration, 2011.

[12] D. Hambling, "GPS chaos: How a $30 box can jam your life," *NewScientist,* 6 Mar 2011.

[13] "Massive GPS Jamming Attack by North Korea," *GPS World,* 8 May 2012.

[14] "GPS jamming: No jam tomorrow," *The Economist,* 12 Mar 2011.

[15] T. Nighswander, B. Ledvina, J. Diamond, R. Brumley and D. Brumley, "GPS software attacks," in *Proc. ACM Conf. on Computer and Communications Security*, Raleigh, North Carolina, USA, 2012.

[16] H. L. van Trees, Detection, Estimation, and Modulation Theory (Part I), Wiley, 1967.

[17] S. M. Kay, Fundamentals of statistical signal processing Volume 2: Detection theory, Prentice-Hall, 1998.

[18] H. Urkowitz, "Energy detection of unknown deterministic signals," *Proc. IEEE,* vol. 55, p. 523–531, April 1967.

[19] A. Sonnenschein and P. M. Fishman, "Radiometric detection of spread-spectrum signals in noise of uncertain power," *IEEE Trans. Aerosp. Electron. Syst.,* vol. 28, no. 3, pp. 654-660, 1992.

[20] R. Tandra and A. Sahai, "SNR Walls for Signal Detection," *IEEE J. Sel. Topics Signal Process.,* vol. 2, no. 1, pp. 4-17, 2008.

[21] A. Balaei and A. Dempster, "A statistical inference technique for GPS interference detection," *IEEE Trans. Aerosp. Electron. Syst.,* vol. 45, no. 4, p. 1499–1511, Oct. 2009.

[22] A. Tani and R. Fantacci, "Performance evaluation of a precorrelation interference detection algorithm for the GNSS based on nonparametrical spectral estimation," *IEEE Systems Journal,* vol. 2, no. 1, pp. 20-26, Mar. 2008.

[23] A. Ndili and P. Enge, "GPS receiver autonomous interference detection," in *Proc. IEEE/ION Position Location and Navigation Symposium (PLANS)*, 1998.

[24] H. Borowski, O. Isoz, F. M. Eklöf, S. Lo and D. Akos, "Detecting False Signals with Automatic Gain Control," *GPS World,* vol. 23, no. 4, pp. 38-43, Apr 2012.

[25] R. Calcagno, S. Fazio, S. Savasta and F. Dovis, "An interference detection algorithm for COTS GNSS receivers," in *Proc. ESA Workshop on Satellite Navigation Technologies (NAVITEC)*, Noordwijk, The Netherlands, 2010.

[26] A. T. Balaei, A. Dempster and J. Barnes, "A novel approach in detection and characterization of CW interference of GPS signal using receiver estimation of C/No," in *Proc. IEEE/ION Position Location and Navigation Symposium (PLANS)*, San Diego, California, USA, 2006.

[27] K. Sheridan, Y. Ying and T. Whitworth, "Pre- and postcorrelation GNSS interference detection within software defined radio," in *Proc. ION GNSS*, Nashville, Tennessee, USA, 2012.

[28] F. Faurie and A. Giremus, "Bayesian detection of interference in satellite navigation systems," in *Proc. IEEE Int. Conf. on Acoustics, Speech, and Signal Process. (ICASSP)*, Prague, Czech Republic, 2011.

[29] M. Psiaki, B. O'Hanlon, J. Bhatti, D. Shepard and T. Humphreys, "GPS spoofing detection via dual-receiver correlation of military signals," *IEEE Trans. Aerosp. Electron. Syst.,* to appear.

[30] M. Psiaki, B. O'Hanlon, J. Bhatti, D. Shepard and T. Humphreys, "Civilian GPS spoofing detection based on dual-receiver correlation of military signals," in *Proc. ION GNSS*, Portland, Oregon, USA, 2011.

[31] P. Montgomery, T. Humphreys and B. Ledvina, "A multiantenna defense: Receiver-autonomous GPS spoofing detection," *InsideGNSS,* vol. 4, no. 2, pp. 40-46, 2009.

[32] J. Nielsen, A. Broumandan and G. Lachapelle, "GNSS spoofing detection for single antenna handheld receivers," *NAVIGATION,* vol. 58, no. 4, pp. 335-344, 2011.

[33] A. Broumandan, A. Jafarnia-Jahromi, V. Dehghanian, J. Nielsen and G. Lachapelle, "GNSS spoofing detection in handheld receivers based on signal spatial correlation," in *Proc. IEEE/ION Position Location and Navigation Symposium*, Myrtle Beach, South Carolina, USA, 2012.

[34] M. L. Psiaki, S. P. Powell and B. W. O'Hanlon, "GNSS Spoofing Detection: Correlating Carrier Phase with Rapid Antenna Motion," *GPS World,* no. 6, pp. 53-58, June 2013.

[35] M. L. Psiaki, S. P. Powell and B. W. O'Hanlon, "GNSS Spoofing Detection Using High-Frequency," in *ION GNSS+*, Nashville, TN, USA, 2013.

[36] E. Axell, G. Leus, E. G. Larsson and H. V. Poor, "Spectrum sensing for cognitive radio: State-of-the-art and recent advances," *IEEE Signal Process. Mag.,* vol. 29, no. 3, pp. 101-116, 2012.

[37] M. Jones, "The civilian battlefield: Protecting GNSS receivers from interference and jamming," *InsideGNSS,* vol. 6, no. 2, pp. 40-49, 2011.

[38] "Ettus research home page," [Online]. Available: http://www.ettus.com/. [Accessed 02 10 2013].

[39] [Online]. Available: https://www.ettus.com/content/files/07495_Ettus_N200-210_DS_Flyer_HR.pdf. [Accessed 02 10 2013].

[40] [Online]. Available: https://www.ettus.com/product/details/WBX.

[41] E. Axell, F. M. Eklöf, M. Alexandersson, P. Johansson and D. M. Akos, "Jamming Detection in GNSS Receivers: Performance Evaluation of Field Trials," in *ION GNSS+*, Nashville, TN, USA, 2013.

[42] F. Bastide, E. Chatre and C. Macabiau, "GPS interference detection and identification using multicorrelator receivers," in *Proc. ION GPS*, Salt Lake City, Utah, USA, 2001.

[43] M. Pini, M. Fantino, A. Cavaleri, S. Ugazio and L. L. Presti, "Signal quality monitoring applied to spoofing detection," in *Proc. ION GNSS*, Portland, Oregon, USA, 2011.

[44] F. Dovis, X. Chen, A. Cavaleri, K. Ali and M. Pini, "Detection of spoofing threats by means of signal parameters estimation," in *Proc. ION GNSS*, Portland, Oregon, USA, 2011.

[45] D. Borio, L. L. Presti and P. Mulassano, "Digital spectral separation coefficient (SSC) for GNSS signal to noise measurements and interference detection," in *Proc. ION GNSS*, Fort Worth, Texas, USA, 2006.

[46] L. Marti and F. van Graas, "Interference detection by means of the software defined radio," in *Proc. ION GNSS*, Long Beach, California, USA, 2004.

[47] F. Bastide, D. Akos, C. Macabiau and B. Roturier, "Automatic Gain Control (AGC) as an Interference Assessment Tool," in *Proc. International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GPS/GNSS),*, Portland, Oregon, USA, 2003.

[48] *CTL-3500 GPS L1 Interference Monitor,* Chronos Technology.

[49] *J-ALERT User's Guide, Models JA-2020 & JA-2030.*

[50] *u-blox 6 Receiver Description,* 2011.

[51] H. L. van Trees, "Detection, Estimation, and Modulation Theory (Part I)," Wiley, 1967.

FOI, Swedish Defence Research Agency, is a mainly assignment-funded agency under the Ministry of Defence. The core activities are research, method and technology development, as well as studies conducted in the interests of Swedish defence and the safety and security of society. The organisation employs approximately 1000 personnel of whom about 800 are scientists. This makes FOI Sweden's largest research institute. FOI gives its customers access to leading-edge expertise in a large number of fields such as security policy studies, defence and security related analyses, the assessment of various types of threat, systems for control and management of crises, protection against and management of hazardous substances, IT security and the potential offered by new sensors.

FOI
Defence Research Agency
SE-164 90 Stockholm

Phone: +46 8 555 030 00
Fax: +46 8 555 031 00

www.foi.se