

Performance analysis of assisted-GNSS receivers

Nicolas Couronneau

Clare Hall



UNIVERSITY OF
CAMBRIDGE

February 2013

A dissertation submitted for the degree of Doctor of Philosophy

Declaration

This dissertation is the result of work carried out in the Astrophysics Group of the Cavendish Laboratory, Cambridge, between October 2009 and February 2013. The work contained in the thesis is my own except where stated otherwise. No part of this dissertation has been submitted for a degree, diploma or other qualification at this or any other university. The total length of this dissertation does not exceed sixty thousand words.

Acknowledgements

I would like to thank my supervisor, Dr Peter J. Duffett-Smith, for his enthusiasm and friendship during my PhD. I have been extremely lucky to work with Peter. He gave me a great deal of freedom during my research, while always boosting my confidence to pursue my work when things did not work as expected. I have developed a lot of my academic and professional skills during my conversations with Peter. He also understood perfectly the “special needs” of a mature research student.

I want to thank Cambridge Silicon Radio for generously sponsoring my research. The guidance and support I received from Stephen Goodwin, Nicolas Graube, Murray Jarvis, and Ben Tarlow were very much appreciated and I would like to thank them again for the time they spent with me. Ramsey Faragher and Sasha Mitelman were instrumental in nurturing my interest in satellite navigation research and their expertise was very much appreciated throughout my PhD work.

I am very grateful to Professor Gérard Lachapelle for inviting me to the Position, Location, And Navigation group at the University of Calgary. My stay in the PLAN group was relatively short but extremely valuable, in particular thanks to the expert advice of Ali Broumandan, James Curran, and Tao Lin.

I had some great times at the Cavendish, in particular thanks to Alex and Michel who have helped me stay motivated during these years.

I thank my college, Clare Hall, for contributing to my funding, which allowed me to present at international conferences.

It is easy to forget how lucky one is to have a supportive and caring family, and I would like to say «Merci Jean-Louis, Maryse, and Cécile» for all their efforts over the years.

Finally, nothing would have been possible without the constant support, patience, and love from my wife, Karen.

Summary

The goal of this thesis is to improve the understanding of the performance of Global Navigation Satellite System (GNSS) receivers that use assistance data provided by cellular networks. A typical example of such a receiver is a mobile phone including a Global Positioning System (GPS) receiver. Using assistance data such as an accurate estimate of the GPS system time is known to improve the availability and the time-to-first-fix performance of a GNSS receiver. However, the performance depends on the architecture of the cellular network and may vary significantly across networks. This thesis presents three new contributions to the performance analysis of assisted-GNSS receivers in cellular networks.

I first introduce a mathematical framework that can be used to calculate a theoretical lower bound of the time-to-first-fix (TTFF) in an assisted-GNSS receiver. Existing methods, for example the flow-graph method, generally focus on calculating the theoretical mean acquisition time of a pseudo-noise signal for one satellite only. I extend these methods to calculate the full probability distribution of the joint acquisition of several satellites, as well as the sequential acquisition of satellites, which is commonly performed in assisted receivers. The method is applied to real measurements made in a multipath fading channel.

I next consider time assistance in unsynchronised cellular networks. It is often argued that unsynchronised networks can not provide fine-time aiding since they do not have a common clock, although few experimental results have been reported in the existing literature. I carried out experiments on a GSM network, a second-generation cellular network, in Cambridge, UK, in order to measure the time stability of the synchronisation signals. The results showed a large variability in the time stabilities across different base stations and I evaluated the performance of an ensemble filter that combines the measurements into a single, more accurate, estimate of the universal time. The main contribution is to show that the performance of such a filter is adequate to provide fine-time assistance to a satellite navigation receiver.

Finally, I address the positioning performance of an assisted receiver in synchronised cellular networks. Cellular positioning has been often investigated in the literature, but few results on real networks have been presented. Many positioning methods are proprietary and little information about their performance in real networks have been published publicly. A CDMA2000 cellular network in Calgary, Canada, was used to collect experimental data. The time stability and the synchronisation of the CDMA2000 pilot signals were excellent and were used to evaluate the performance of CDMA2000-based cellular positioning system. I then developed a method to combine the pseudo-range measurements from the GPS signals and the CDMA2000 base stations. I evaluated the performance of positioning in both outdoor and indoor environments, and I analysed the effects and the possible mitigation of non-line-of-sight signals. The main contribution is to show that additional satellite navigation signals can improve the accuracy of cellular positioning beyond what is theoretically expected from the improvement in the geometry.

Contents

Declaration	3
Acknowledgements	5
Summary	7
Contents	9
1 Introduction to radio positioning systems	15
1.1 Fundamentals of positioning systems	15
1.2 Global navigation systems	23
1.3 Positioning in cellular networks	28
1.4 Thesis outline	32
2 Estimation and detection in navigation receivers	35
2.1 Parameter estimation	36
2.2 Signal detection	44
2.3 Acquisition of GNSS signals	46
2.4 Position estimation	50
2.5 Assisted-GNSS receivers	53
2.6 Summary	56
3 Analysis of the time-to-first-fix in assisted-GNSS receivers	59
3.1 Analysis of the acquisition of direct-sequence spread spectrum signals .	60
3.2 Mean features of assisted-receivers models	68
3.3 Acquisition model of an assisted receiver	72
3.4 Illustration for typical signals	77
3.5 Application to real signals	79
3.6 Conclusions and future work	89

4	Time assistance from unsynchronised cellular networks	93
4.1	Introduction	94
4.2	Overview of GSM signals	96
4.3	Oscillator models and time estimation	101
4.4	Time stability of the GSM air interface	105
4.5	Prediction of time deviations	116
4.6	Tracking of local oscillator bias	123
4.7	Discussion and conclusions	131
5	GNSS aiding in synchronised cellular networks	135
5.1	Introduction	136
5.2	Measurements of times of arrival of CDMA2000 signals	138
5.3	Time stability and synchronisation of CDMA2000 networks	144
5.4	Error analysis of the propagation time	148
5.5	Positioning using cellular signals only	157
5.6	Positioning using GNSS and cellular signals	166
5.7	Discussion	172
5.8	Conclusions	175
6	Conclusions	177
6.1	Summary of contributions	177
6.2	Future work	178
A	GPS software receiver	181
A.1	Acquisition	181
A.2	Tracking	182
B	CDMA2000 Sync Channel Message	185
B.1	Physical channel	185
B.2	Frames and super-frames	186
B.3	Sync Channel Message structure	186
	References	189

Nomenclature

C/N_0	carrier-to-noise-density ratio
3GPP	3 rd Generation Partnership Project
3GPP2	3 rd Generation Partnership Project 2
AFLT	Advanced Forward-Link Trilateration
AMPS	Analogue Mobile Phone System
AWGN	Additive White Gaussian Noise
BSC	Base Station Controller
BSIC	Base Station Identity Code
BTS	Base Transceiver Station
C/A	Coarse/Acquisition
CEP	Circular Error Probable
CRLB	Cramér-Rao Lower Bound
DFT	Discrete Fourier Transform
DOP	Dilution Of Precision
DSSS	Direct-Sequence Spread Spectrum
ETSI	European Telecommunications Standards Institute
FCC	Federal Communications Commission
FDMA	Frequency-Division Multiple Access
FFT	Fast Fourier Transform
GLONASS	Globalnaya Navigatsionnaya Sputnikovaya Sistema
GLRT	Generalised Likelihood-Ratio Test
GMSK	Gaussian Minimum Shift Keying

GPS Global Positioning System

GSM Global System for Mobile communications – initially Groupe Spécial Mobile

ICD Interface Control Document

IGS International GNSS Service

IP Internet Protocol

ITU International Telecommunication Union

LBS Location-based service

LMU Location Measurement Unit

LOS Line Of sight

LRT Likelihood-Ratio Test

LTE Long-Term Evolution

MS Mobile Station

NIS Normed Innovation Squared

NLOS Non Line Of Sight

OCXO Oven-Controlled Crystal Oscillator

PGF Probability Generating Function

ppb parts-per-billion

ppm parts-per-million

PRN Pseudo-Random Noise

PSTN Public Switched Telephone Network

RMS Root Mean Square

RSS Received Signal Strength

SAGE Space-Alternating Generalised Expectation-Maximisation

SCHM Sync Channel Message

SIC Successive Interference Cancellation

TCXO Temperature-Compensated Crystal Oscillator

TDMA Time-Division Multiple Access

TTFF Time-To-First-Fix

TTFH Time-To-First-Hit

UTC Coordinated Universal Time

UTM Universal Transverse Mercator

UWB Ultra-wide bandwidth, or ultra-wide band

Introduction to radio positioning systems

Radio positioning systems and cellular networks have changed our lives in ways that may not have been possible to predict. Global navigation satellite systems (GNSSs), and in particular the Global Positioning System (GPS), have brought positioning to entry-level mobile devices, with an accuracy that was once only available to military personnel and surveyors. Some of these devices, for example mobile phones, have also access to the Internet using a cellular network. The combination of position information and access to the Internet has paved the way to applications that are developed around the user position. The new possibilities cover road charge payment, gaming, personal navigation, etc.

1.1 Fundamentals of positioning systems

Several methods and systems have been developed in order to determine one's position. Some systems work in a local area while others operate globally; some rely on a dedicated infrastructure while others work in an unprepared environment; some work with radio-frequency signals while others rely on optical measurements, etc. The classification of these methods is thus challenging, yet also desirable in order to understand the landscape of possible positioning systems. We review some of the most common technologies in this section, with a particular focus on radio-frequency systems.

Methods based on propagation time

Most radio-positioning systems measure the range between a transmitter and a receiver. In the following, we assume that the measurements are performed between one receiver and N transmitters; the analysis is also valid for the converse situation, with one transmitter and several receivers. The user position, \mathbf{x} , is related to its distance r_i to the transmitter i at position \mathbf{x}_i via the system of equations

$$\begin{cases} r_1 = \|\mathbf{x}_1 - \mathbf{x}\| \\ \vdots \\ r_N = \|\mathbf{x}_N - \mathbf{x}\|, \end{cases}$$

where $\|\mathbf{v}\|$ denotes the Euclidean norm of the vector \mathbf{v} , i.e. $\|\mathbf{v}\| = \sqrt{v_x^2 + v_y^2}$ for a vector \mathbf{v} or Cartesian coordinates $[v_x, v_y]$. We assume perfect measurements of time of flights in this section and we address the case of noisy measurements in Section 2.4.

We now calculate the ranges from the measurements of propagation times. We assume the signal is carried by an electromagnetic wave that propagates at the speed of light in vacuum, $c = 299\,792\,458$ m/s. The signal is sent by transmitter i at time TOT_i and is received by the user at time TOR_i , from which we can calculate the range, r_i , using the relationship $r_i = c (\text{TOR}_i - \text{TOT}_i)$. The receiver clock must be synchronised with the transmitter in order to measure TOR in the same time scale as TOT_i . The signal carried by an electromagnetic wave “travels” about 3 m in 10 ns, hence the time synchronisation between the receiver and the receiver must be of the order of the nanosecond. Such a synchronisation accuracy is challenging and not feasible in mass-market devices, specially when they operate in an environment with changing temperatures. The synchronisation issue is a common problem in radio positioning systems. It is, however, less problematic in systems with slower propagation speeds, such as underwater Sonars or ultrasonic beacons that use acoustic waves.

We can modify the system of equations for the situation where all the transmitters are synchronised together and the receiver operates in a different, local, time scale. The modification consists of adding the *user bias*, b_u , which is the time difference between the time scale of the transmitters and the time scale of the receiver. We now have $r_i/c = \text{TOR}_i^{\text{RX}} - \text{TOT}_i + b_u$, where TOR_i^{RX} is the reception time in the receiver time scale. The *pseudo-range*, ρ_i , is often used and is defined as

$$\rho_i = c (\text{TOR}_i^{\text{RX}} - \text{TOT}_i).$$

The pseudo-range is more convenient to work with as it directly relates to the measurements made by the receiver, in its local time scale. The previous system of equations

can be written using the pseudo-range, giving

$$\begin{cases} \rho_1 = \|\mathbf{x}_1 - \mathbf{x}\| - c b_u \\ \vdots \\ \rho_N = \|\mathbf{x}_N - \mathbf{x}\| - c b_u. \end{cases} \quad (1.1)$$

Equation 1.1 is often called the *position equation* and is fundamental in positioning systems using radio signals. A common method to solve the position equation with noisy measurements is presented in Section 2.4. The equation is presented in its time-of-arrival (TOA) form, where all the pseudo-range times, ρ_i/c , are measured from the origin of the receiver time scale.

Another possibility is to use only time-differences, which does not require the receiver time scale to have a time origin – only time differences are required. This approach is called time-difference of arrival (TDOA). The system of N equations to solve is then

$$\begin{cases} \rho_2 - \rho_1 = \|\mathbf{x}_2 - \mathbf{x}\| - \|\mathbf{x}_1 - \mathbf{x}\| \\ \vdots \\ \rho_N - \rho_{N-1} = \|\mathbf{x}_N - \mathbf{x}\| - \|\mathbf{x}_{N-1} - \mathbf{x}\|. \end{cases} \quad (1.2)$$

The user bias is not an unknown variable as it does not appear in Equation 1.2, which is normal since the TDOA relies on time differences only.

Both the TOA equation (Equation 1.1) and the TDOA equation (Equation 1.2) solve the same problem and require the same number measurements. The TOA approach is also known as *trilateration* and the TDOA approach as *multilateration*. The locii of the positions in a two-dimensional TOA problem are circles and they are hyperbolas in a TDOA problem. This name sometimes leads TDOA-based systems to be called *hyperbolic positioning*. In Section 2.4, we will see that, with noisy measurements, the solution to the TOA system of equations is generally more robust than for a TDOA system.

However, the TDOA approach may be more practical in some applications. The time differences can be easily calculated by the cross-correlation of two signals carrying the same pattern without knowing the pattern beforehand. This situation arises when locating the source of radio-frequency interference, for example. The content of the interfering signal is generally unknown, however the same signal can be received from different locations. The signals received at the various locations can be cross-correlated in order to calculate the time differences, and the source of the interference can be localised by solving the TDOA equation. The content of *signals of opportunity*, such as

television and radio broadcasting, are generally unknown yet they are synchronised, which makes them suitable for TDOA-based positioning. A receiver with a TOA capability is more complicated since a local copy of the signal pattern is needed in order to calculate the times of arrival.

The synchronisation of the transmitters is not always possible, in particular if they have not been designed as a positioning system. Some cellular signals, for example, carry voice and data to mobile phone users, without synchronisation between the receiver and transmitter. A first possibility is to use dedicated equipment to measure the time biases of the different transmitters, and send the corrections to the mobile, as proposed by Duffett-Smith *et al.* (1992). However, dedicated equipments increase the cost of the system. Methods such as Matrix, described by “Radio positioning systems” (2003) and “Radio positioning systems” (2008), have been proposed to solve the problem of unsynchronised receivers without relying on external equipment. The Matrix method is described in Section 1.3. A system similar to Matrix has been proposed by Neven *et al.* (2005) in order to synchronise several receivers for the automatic dependent surveillance-broadcast (ADS-B) system, and air traffic monitoring system.

Other radio-frequency methods

We now present some radio-frequency techniques that do not rely on the measurement of the signal propagation times. These alternative methods can be interesting in mass-market applications since the accurate measurement of times can be technically challenging.

Measuring the signal strength at the receiver location is one of the first radio-positioning method designed. A path-loss model is used to calculate the signal power as a function of the distance. A common path-loss model is $P(d) = \alpha P_0 d^{-n}$, where $P(d)$ is the power of the signal received at a distance d , for a transmitted signal of power P_0 ; α is a coefficient which is a function of the frequency and antenna gain; and n is the path-loss exponent, which depends on the propagation environment. The accuracy of the received signal strength (RSS) method is generally low. Uncertainties in the value of the path-loss exponent and in the transmitted power, added to the time-varying propagation conditions of the channel, affect the reliable estimation of the distance d . For example, Alexander (1983) reports values of n between 1.4 and 6.5, a range of possible values so wide that it leads to a large uncertainty in the range estimation. Nevertheless, this method has enjoyed some popularity as the signal strength is generally reported by devices, even if they have not been designed with a positioning capability. RSS is thus potentially available on a large variety of platforms.

Angle-of-arrival (AOA) methods use the angles between the user and some reference points in order to calculate the position. These methods are sometimes called radio-direction finding and the AOA position equation is solved by *triangulation*. Measuring the angle generally requires a specially designed antenna and a phased-array antenna is sometimes used. AOA methods are commonly utilised from positioning in cellular networks. The radiation pattern of cellular networks antennas is often about 120° , which leads to a division of each cell in 3 angular sectors. The base stations can then determine the angles of arrivals of the signals from the mobile device with an uncertainty of 120° . Despite the large uncertainty in the arrival angle measurements, several base stations may be in view of the same mobile device, thus increasing the accuracy of the positioning. Navigation aids for aircraft also use AOA methods. Non-directional beacons (NDB), for example, continuously transmit RF signals that are received by an automatic direction finder (ADF) onboard aircraft. The pilot reads the bearings of different beacons on the ADF, and then calculates his position by triangulation.

Fingerprinting is a method particularly suited for positioning with signals that have not be designed for that usage. It is generally a two-stage process. An area is first surveyed in order to record a “fingerprint” of signals, which is the summary of the interesting features of a signal, such as the signal strengths, the waveform patterns, etc. at known locations. The user then determines his position by finding a match of the “fingerprints” of the received signals with existing records in the database. Bahl *et al.* (2000) present one of the first evaluations of indoor positioning using the fingerprinting of WiFi signals. They used the signal strengths of WiFi access points as a fingerprint and they reported a median positioning error better than 5 m. Because fingerprinting often relies of the received signal strength, it suffers from the same problems as RSS techniques. Elnahrawy *et al.* (2004) present experimental results of several fingerprinting algorithms. They highlight that neither increasing the sampling resolution during the survey, nor improving the algorithms, leads to a significant improvement in the position accuracy. These observations suggest that fingerprinting methods can not achieve high accuracy, although such methods may be cost-effective in some applications as they do not require modification of the infrastructure.

Finally, Cell-ID is a popular method of obtaining coarse positioning. It identifies transmitters of known positions near a mobile station and calculates the position of the mobile station, generally as a weighted average of the position of the transmitters. This method is particularly common for positioning in cellular networks. It is similar to fingerprinting but it is usually considered to be a separate technique, mostly because it does not require surveying but it necessitates some knowledge of the network

operations in order to identify the transmitters and their positions. On the other hand, fingerprinting is generally possible using signals of opportunity, without knowing the locations of the transmitters. Several databases have been built and contain the identities and locations of cellular base stations. Cell-ID is a widespread method but it is not as prevalent in the academic literature as some other methods, possibly because it often relies on proprietary databases. The position accuracy is low; Trevisani *et al.* (2004) measured average errors between 500 m in an urban centre in Italy and 1 km on a highway in the United States.

Effects of radio propagation on positioning

Positioning with radio signals generally relies on the arrival times or the amplitude of the signals. These two parameters are affected by the propagation conditions of the radio waves. The degradation of radio signals is commonly the result of multipath propagation, which is the propagation of radio waves along more than one path.

A first consequence of multipath propagation is *multipath fading*. The radio waves that arrive at the receiver antenna from different paths are not necessarily in phase, since each path introduces a different group delay. The recombination of radio waves with random phases can be additive or subtractive, thus modifying the amplitude of the resulting wave. Multipath fading has been studied extensively, in particular in personal mobile communications, and several models of fading have been developed for different environments. Hashemi (1993) provides a survey of theoretical models and experimental results in indoor environments, where the most severe conditions of radio propagation occur. The relative phase differences of the paths are variable in a dynamic environment, hence the amplitude of the recombined wave at the receiver varies with time. The path lengths are often affected by road traffic, surfaces moved by the wind, etc. and, in practice, the fading is almost always time-varying. Fading often occurs over distances which are of the order of the carrier wavelength. This property can be exploited to mitigate the effect of signal fading by using *spatial diversity* methods. These techniques consist of receiving the signal at more than one location, using more than one antenna, such that a subtractive combination at one location can be compensated by an additive combination at another. Spatial diversity is often used in radio-communications and it is also present in some GNSS receivers, in particular in automotive applications. Multipath propagation can also change the polarisations of the radio waves, hence antennas with different polarisation profiles are also used in diversity methods.

Another consequence of multipath propagation is the degradation of the accuracy

of the time measurements. We have seen previously that positioning systems generally require the propagation times of the line-of-sight (LOS) signals in order to calculate the position. The signal from the LOS path may not be detected reliably in a multipath channel if the combination of waves from non-line-of-sight (NLOS) paths produces a stronger signal. This cause of degradation is often implied in the GNSS community when multipath is mentioned. Multipath fading also affects GNSS receivers, in particular during the acquisition of the signals, but it has less important consequences on the positioning accuracy. Multipath propagation is notoriously difficult to mitigate. A classical illustration is to consider the reception of satellite signals in urban centres with tall buildings, a situation called an *urban canyon*. The multiple reflections of the signals on the vertical surfaces of the buildings, combined with the masking of the satellites, can lead to significant position errors for personal navigation. This problem is addressed by Groves (2011), among others, who addresses the problem of locating on which side of a street the user is.

Stand-alone positioning systems

Many radio-positioning systems are limited by their reliance on previously deployed facilities, for example satellites or radio-frequency beacons. This dedicated equipment has development, deployment, and maintenance costs which can outweigh the benefits of bringing positioning capabilities. Radio-positioning systems also have physical limitations. As an example, we will see in Chapter 5 how multipath propagation and signal attenuation reduce the availability of radio-positioning inside buildings. Similarly, positioning a robot underwater or in a mining site may not be possible using radio-based methods. Additionally, a radio-positioning system may be subject to interference, intentional or not, which may completely disrupt its availability. We wish to develop positioning and navigation systems that can operate in unprepared environments or that are not limited by the constraints of radio-propagation.

Vision has been frequently used in positioning technologies. Historically, sailors used the positions of stars to determine their vessels' positions, a technique then adopted by early pilots. Celestial navigation is based on the observations of the angles of known stars, using a sextant for example. The position is then calculated using a star almanac and the time of the measurements. Celestial navigation is seldom used nowadays, except to determine the attitude – not necessarily the position – of a spacecraft. Visual odometry, another vision-based method, consists in estimating the motion of a camera by tracking the motion of visual features over time. The trajectory of the features gives the mobile's velocity vector, which is then integrated to calculate the

position. Some amount of diversity in the images is required in order to find enough features with a geometry that allows the calculation of the motion. It is also possible to use known features or recognize objects in order to obtain absolute positions. Vision is often used in robotics for local path planning and obstacle avoidance, as used by Thrun *et al.* (2006) during the navigation “Grand Challenge” of the American Defense Advanced Research Projects Agency (DARPA). It is not a positioning task as such, although it can provide location information of obstacles in a local area.

An active area of research concerns the navigation of a mobile in an unprepared and unknown environment. Known as simultaneous localisation and mapping (SLAM), these techniques contrive to build a map of unknown surroundings at the same time as positioning the mobile in it. It is, in general, a highly computational problem and many techniques have been proposed to simplify this task. Newman *et al.* (2009) present the results of a visual SLAM system that achieves a position error better than one metre. Recently, Faragher *et al.* (2012) proposed a method of SLAM in an office building using radio-frequency signals of opportunity, accelerometers and magnetometers from a smartphone, and a foot-mounted accelerometer.

Inertial navigation systems were one of the first standalone solutions developed. They are based on the measurement of the acceleration vector and the rotation rates of the user. These derivatives of the user motion can be integrated to calculate the user’s change of position. Inertial systems were initially expensive and reserved to specific applications, such as aircraft and missile guidance. Microelectromechanical systems (MEMS) have lowered the cost of inertial sensors and inertial measurement units (IMUs) are now gaining popularity in commercial products. Inertial systems are commonly found in commercial and military aircraft, ships, and submarines.

Sensor fusion

The measurements from different systems are often combined in order to improve the position accuracy. Inertial measurements units, for example, are affected by the biases of their sensors, which create a drift of the user position as the biases are integrated. For this reason, IMUs are commonly supplemented with GNSS measurements. The GNSS signals bring high accuracy and global positioning, whereas the IMU measurements bring robustness to the system when the RF signals become unavailable. Inertial positions can also be calculated at a higher rate than GNSS positions, hence the coupling of an IMU and a GNSS receiver is particularly attractive for platforms with large dynamics. Similarly, the combination of Cell-ID, fingerprinting, and RSS can be used to

estimate the position of a cellular device without changing the network infrastructure or the receiver. This approach is often used for positioning on smartphones.

Sensor fusion is a major topic in navigation systems research. It is based on Bayesian probabilistic methods to combine noisy information from several sensors. A major building block of sensor fusion is the method developed by Kalman (1960), now commonly called Kalman filter, which is presented in Chapter 2. There are several other tools inspired by the original Kalman filter, which can deal with non-linearities and non-Gaussian noises, for example. Some challenges of modern sensor fusion include the characterisation of the sensor noises and failure modes, the modelling of the mobile platform dynamics, the development of efficient algorithms for real-time operations on mass-market devices, etc. I have used an approach similar to sensor fusion in Chapter 4, in order to improve the time stability of a receiver.

1.2 Global navigation systems

History

Radio positioning systems were developed in the 1940s to help the positioning of ships and aircraft. One of the first global systems was the LOnG RAnge Navigation, LORAN-A, system. Synchronised transmitters periodically sent radio-frequency signals in a low-frequency band, at about 100 kHz. The user measured the time differences between the arrival times of pairs of signals and used these to calculate his position. The typical accuracy was about 200 m, although this could be degraded inland. The LORAN-A system was extended to form the LORAN-C systems (United States Coast Guard, 1994), which was used for marine and air navigation until it was decommissioned in 2010 in the United States. The General Lighthouse Authorities (GLA) of the United Kingdom have promoted eLoran (enhanced-LORAN), which improves the performance of LORAN-C and facilitates its integration with satellite navigation systems. The OMEGA system (Kasper *et al.*, 1978) was a radio navigation system whose principles were similar to LORAN-C. It used very low-frequency signals, between 10.2 and 13.6 kHz, which provided worldwide coverage but had less accuracy than LORAN-C. It was decommissioned in 1997 by the United States. DECCA was a British navigation system similar to LORAN that was developed during World War II. Stations transmitted a continuous signal at low frequency and the user measured the phase differences of the RF signals. The system was shut down in 2000. LORAN, OMEGA, and DECCA operated using the measurements of time or phase differences and therefore were hyperbolic positioning systems.

Terrestrial systems such as LORAN, DECCA, and OMEGA, have shortcomings. The transmitters are located in the same horizontal plane, a geometry that can not provide useful altitude information. The horizontal propagation of the radio waves also encounters several obstacles inland and is affected by built-up areas, which degrades the position accuracy. Furthermore, low-frequency signals are better suited for long-range propagation, but high-frequency signals provide better accuracy.

These shortcomings led to the development of satellite navigation systems. The first satellite navigation system was the United States Navy Navigation Satellite System (NNSS), more commonly known as Transit. A user would monitor the Doppler shift of the Transit radio-frequency carrier in order to calculate his position. The constellation was small and only one satellite was in view of the user in general. This geometry did not allow the calculation of the position immediately and the user often had to wait until enough Doppler measurements had been collected from different points of a satellite orbit before the position equation could be solved. The American Department of Defense (DOD) formed a working group in 1973 and started developing what became the Global Positioning System (GPS).

The Global Positioning System

The Global Positioning System is arguably the most commonly-used global navigation satellite system (GNSS). It operates by measuring the propagation times of radio-frequency signals sent by satellites. The GPS satellites continuously broadcast signals whose transmission times are synchronised across all satellites. The user can then calculate his position using the TOA method. The time stability and synchronisation of the transmitted signals is excellent, thanks to the use of atomic clocks onboard the satellites and monitoring by ground-based stations that upload time corrections to the satellites. The high stability of the signals is exploited by many timing applications that do not always require the positioning capabilities of GPS, for instance to synchronise equipments separated by large distances.

The Global Positioning System is described in several references, including the books by Parkinson *et al.* (1996) and the website of the National Coordination Office for Space-Based Positioning, Navigation, and Timing (2012). The ground segment is operated by the United States Air Force and is composed of several command and monitoring stations across the world. The space segment comprises a constellation of satellites that ensures worldwide coverage – between 24 and 31 operational satellites in general. The satellites orbits are quasi-circular, with a radius of 26 000 km, resulting in an orbital period of 12 h in sidereal time. The signals are transmitted using a direct-

sequence spread spectrum (DSSS) technique. This method modulates the original signal with a pseudo-random noise (PRN) sequence. The binary elements of a PRN sequence are called *chips*. They are often generated by a linear feedback shift register.

GPS satellites transmit two signals with different PRN characteristics. The coarse acquisition (C/A) code is transmitted on the frequency link 1 (L1), whose carrier frequency is 1575.42 MHz. It has a chipping rate of 1.023 Mchips/s and a length of 1023 chips, thus the period of the C/A code, T_{CA} , is 1 ms. The precision (P) code is spread at a ten times faster chipping rate. It is transmitted on the L1 frequency, in quadrature to the C/A code, and also on the frequency link 2 (L2), at 1227.60 MHz. The P code is encrypted to form the Y code, often called the P(Y) code. The encryption key is provided by the DOD to authorised users only. The C/A code was intentionally degraded by the selective availability (S/A) feature until May 2000.

The use of DSSS has several advantages. The modulation distributes the power of the original signal across a large spectrum, and the maximum power spectral density can even be below the noise floor of the receiver. This has the advantage of covert operation and it limits the electro-magnetic interference of other equipment, in particular radio-telescopes. The DoD guarantees the L1 C/A signal is received with a strength of at least -183 dBW at the surface of the Earth. This brings the power spectrum density below the noise floor, as illustrated in Figure 1.1.

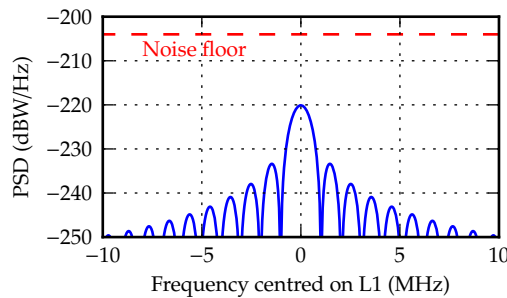


Figure 1.1: Illustration of the power spectrum density of the L1 C/A signal. The noise floor is set to -204 dBW/Hz, a value typical of a terrestrial GPS receiver.

The DSSS modulation also facilitates the measurement of the arrival times. A PRN sequence can be built such that its auto-correlation function has all the signal energy concentrated at a lag of zero, and negligible correlation at any other lag. The receiver can recover the arrival time by correlating the received signal with a local replica of the PRN sequence. The correlation properties of a PRN sequence is illustrated in Figure 1.2. We note that the correlation function becomes zero almost all the time for any distance

large than 300 m from the origin.

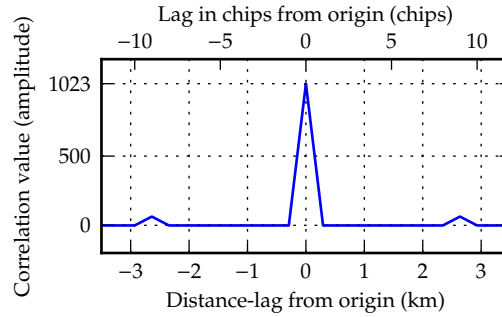


Figure 1.2: Autocorrelation function of the PRN 1 sequence of the C/A code. The correlation values are in the amplitude domain.

Finally, the DSSS modulation provides code-division multiple access (CDMA), a technique that allows several transmitters to share a common radio-frequency carrier without interference. This is achieved by choosing a class of PRN sequences that have little cross-correlation between each other: all the sequences are orthogonal to each other. The family of Gold codes (Gold, 1967) has this property and is used by the GPS L1 C/A signal. All the satellites can transmit on the same frequency and each satellite is identified by its unique PRN code generator. Figure 1.3 illustrates the comparison of the first 100 chips of the PRN 1 and 2 of the C/A code. It can be shown, as in Parkinson *et al.* (1996, chapter 3), that the worst-case of cross-correlation power is about -23.8 dB below the nominal correlation power.

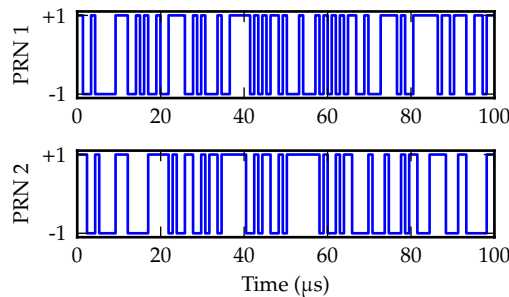


Figure 1.3: First 100 chips of the PRN 1 and PRN 2 sequences of the C/A code.

The signals also carry the GPS navigation message, which is modulated by a binary-phase shift keying modulation at 50 bits/s. The navigation message contains information needed to determine the satellite positions and the times of transmission of the signals with high accuracy. This includes the ephemeris data and the time-of-week

(TOW) counter, which gives the time of transmission of the signal in the GPS system time scale. The ephemeris data provide the orbital elements and correction terms that are required to calculate the position of the satellite at a given time, as well as information about the time deviations of the atomic clocks. The parameters given by the ephemeris are only valid for a short time interval, generally about four hours. The almanac data provide the orbital elements and correction terms with less accuracy than the ephemeris data, but they are valid for several days. The descriptions of the navigation message, the C/A code generators, and the signal specifications are described in GPS interface control document (ICD, GPS Joint Program Office, 2004).

Other Global Navigation Satellite Systems

The GPS L1 C/A signal is undoubtedly the most frequently used GNSS signal at this time. Other nations have developed their own satellite-based systems and these are gaining increasing popularity among receiver manufacturers.

The Russian GLObal NAVigation Satellite System, GLONASS, has been developed initially by the Soviet Union and then by Russia (Russian Institute of Space Device Engineering, 2008). The satellites are identified by their frequencies, instead of a PRN sequence as in the GPS, which creates integration problems in GPS receiver, since the frontends need a wider bandwidth to accommodate both the GPS signals on a fixed carrier frequency and the GLONASS signals at variable central frequencies. Nevertheless, the system is fully operational and its 31 satellites, as of November 2012, offer global coverage. GLONASS broadcast pseudo-noise signals in frequency bands close to those of GPS.

The European Union has been working on the Galileo system (European Union, 2012) and has deployed four in-orbit validation satellites as of November 2012. Galileo has been designed with interoperability with GPS in mind. The Compass system, also called Beidou-2, is being developed by the People's Republic of China. There are currently 16 Compass satellites, but most of the interface control document has not been made public. The GPS system is also going through an upgrade with the addition of new navigation signals. A new civilian signal on the L2 frequency, the L2C signal, has a faster spreading rate than L1 C/A, which can improve the position accuracy. The presence of two civilian signals at different carrier frequencies also facilitates the correction of ionospheric errors.

Satellite augmentation systems provide information that improves the performance of a GNSS receiver, for example the status of a GNSS constellation, the ephemeris, and the clock and ionospheric correction data. The Wide-Area Augmentation System (WAAS)

and the European Geostationary Navigation Overlay Service (EGNOS) are currently in use to broadcast information about the GPS constellation and the GPS L1 C/A signal. The signals are transmitted by geostationary satellites on the L1 frequency.

The current trend is towards receivers capable of operating with signals from multiple systems on several frequencies. Receivers compatible with GPS, Galileo, and Glonass, and operating with signals from two different frequency bands, are commercially available as of 2012.

1.3 Positioning in cellular networks

The wide majority of cellular networks provide the infrastructure for voice and data communications using mobile phones. They have changed the nature of communication between individuals in depth and over a short period of time. The United Kingdom had some 81.6 million mobile subscribers in 2011 according to Ofcom (2012), for a population of 62 million people. Cellular networks originally carried voice only, but mobile devices now offer data services, such as access to the Internet. At the same time, the computing power of the devices has increased and applications that require intense data processing are now widely available on personal handsets. This situation opened new possibilities for positioning capabilities on mobile devices. In this section, we review the main technologies of cellular networks and their positioning possibilities.

History and technology of cellular networks

Different technologies exist and all have in common the division of an area into many cells, each cell being covered by a base transceiver station (BTS). The Shannon-Hartley theorem shows that a communication channel with a given bandwidth and signal-to-noise ratio, such as the radio link between the BTS and the user, has a finite capacity. This can be a problem as the number of users increases in a cell, thus requiring additional capacity. The sizes of the cells change depending on their locations so that the channel capacity is optimised. Other constraints, such as the propagation conditions and technical limitations of the network, also affect the sizes of the cells.

The first cellular systems relied on analogue signals to communicate. The analogue mobile phone system (AMPS), for example, was introduced in the early 1980s, mostly in North America and Australia. The total access communication system (TACS), a variant of AMPS, was used in Western Europe. The deployment and adoption of these early systems was limited and I could not find evidence of any of these networks being still operational in 2012. The second-generation (2G) networks were arguably more popular.

They relied on digital radio communications, with two major technologies dominating the market. The global system for mobile communications (GSM, although originally standing for Groupe Spécial Mobile) is the most common technology in 2G networks. The specifications are maintained by the European telecommunications standards institute, (ETSI, *ETSI website*), and are generally published by the 3rd Generation Partnership Project (3GPP, *3GPP website*). A major feature of this network is that the BTSs need not be synchronised. Each BTS is attributed a set of unique frequencies in its area, hence implementing frequency-division multiple access (FDMA) over the entire network. The users, also called *mobile stations*, communicate with the BTSs over a channel regulated by time-division multiple access (TDMA). The communications occur on a common frequency and at specific time intervals, such that the signals from two mobile stations do not overlap. GSM networks cover more than 90 % of the world's population according to the GSM Association, (*GSM Association website*), a group of companies supporting the GSM standard.

The alternative to GSM among second-generation networks is the IS-95 standard, marketed as cdmaOne. The standard is maintained by the telecommunication industry association (TIA) and is not freely available. One of the main characteristics of the standard, and its biggest architectural difference with GSM, is the requirement for synchronised BTSs. The standard does not have a FDMA component like GSM and all base stations within a network transmit on the same frequency. The absence of interference and the access to the BTSs are assured by code-division multiple access. The signal from each BTS is modulated by a pseudo-noise sequence, similarly to the DS-SS modulation of GPS signals. The base stations are identified by the time offsets of their spreading sequences. This implementation requires a common time scale for all the transmitters, to mark the time origin of the time offsets. The IS-95 standard specified the GPS time scale is to be used, which in practice requires a GPS receiver in time-transfer mode at every BTS site.

The third-generation (3G) standards of cellular communications provide larger bandwidths and better support of data services. They are also divided into two main competitors: the Universal Mobile Telecommunication System (UMTS) has been developed by the 3GPP to succeed to the GSM standard, while the CDMA2000 standard has been built on the foundation of IS-95. UMTS has several differences with the GSM standard. The air interface, which specifies the radio communications between the BTSs and the mobile stations, has two different implementations. The most common is the W-CDMA standard, which is based of code-division multiple access and has a bandwidth of about 5 MHz. The network architecture is, like GSM, unsynchronised,

despite the use of CDMA. The CDMA2000 standard is maintained by and publicly available from the 3rd Generation Partnership Project 2 (3GPP2, not to be confused with 3GPP).

The fourth-generation systems are being deployed but are not as widespread as 3G networks as of 2012. The main technology is the Long-Term Evolution (LTE) standard (3GPP - *LTE*), which affords a larger bandwidth than UMTS. LTE employs orthogonal frequency-division multiple (OFDM) access.

Cellular positioning techniques

The communication industry quickly became interested in knowing the position of mobile device users in cellular networks. User positioning became the cornerstone of a new range of applications, known as location-based services (LBSs). The position is generally presented to the user of the mobile terminal, for example by presenting a map. Other LBSs transmit the position to a third-party, for example to locate an emergency call, to restrict some services to a given geographical area (geo-fencing), or to collect road toll charges. The possibility of obtaining the user's position without consent, or even knowledge, has raised privacy concerns, as illustrated by *Malte Spitz*.

A major driver of research in the positioning of mobile phones is the enhanced-911, or E911 mandate of the Federal Communications Commission (FCC) of the United States. This mandate requires that mobile network operators provide the user position to emergency services during an emergency call (9-1-1 in the United States). The position accuracy requirements are determined by the FCC. They vary with the environment, but are generally in the range of 50 to 150 m. These accuracy targets created a sustained interest in developing accurate and robust positioning methods for cellular devices. Various solutions have been proposed and I review some of literature around this topic. A significant part of the research into positioning methods for commercial devices is performed by private companies and is not always published in the academic literature.

How the position of the user is calculated depends on the peripherals available on the device. We review some of the most common methods and we refer to Gustafsson *et al.* (2005) for a more complete treatment. Klukas (1997) investigated a TOA positioning system for an AMPS network. The network was not synchronised and the author used GPS receivers in order to calibrate the transmitters' clocks. The multipath propagation was mitigated by using the multiple signal classification (MUSIC, Schmidt, 1986) algorithm. The reported root mean square error (RMS) was between 190 m and 290 m in an urban environment.

Positioning with GSM networks is more challenging because the network is not synchronised. Most methods rely on dedicated equipment within the cellular network to measure the time deviations of the signals from the base stations. A solution is the enhanced-observed time difference (E-OTD) of arrival, also called observed time difference of arrival (OTDOA) in UMTS networks. It relies on the presence of location measurement units (LMUs) in the network, which continuously measure the biases of the signals from the BTSs. Drane *et al.* (1998) attained a RMS accuracy of about 150 m in an urban environment, where the timing signals were calibrated.

LMUs need to be located at several points of the network in order to maximise the coverage of the base stations. The deployment and maintenance costs of LMUs can be problematic for network operators. The Matrix system, previously mentioned, is a solution that does not rely on dedicated network equipment. The Matrix technique works in cellular networks, where M receivers at different locations can measure the arrival times of the signals transmitted by N base stations. This method exploits the large number of receivers in common view of a set of transmitters in order to find the unknown time biases of the transmitters. It is then possible to write a system of equations with the biases of all the clocks in the network, both at the receiving terminals and the serving BTSs. The new system of equations can be solved under the condition $MN \geq 3M + N - 1$. Duffett-Smith *et al.* (2001) present the results of experiments in a dense urban environment. The 67-percentile position errors are about 130 m, which is comparable to the GPS errors measured at the same locations in that challenging environment. The advantages of Matrix over GPS are the better availability of the cellular signals and their faster acquisition times. An extension to the Matrix method, called the Solo Matrix system, regularly performs a time calibration of the GSM transmitters using the position and time of a GPS receiver. The position is then calculated using a TDOA approach, assuming the transmitter clocks have not changed. Duffett-Smith *et al.* (2004) show that the short-term time stability of GSM networks is adequate for outdoor positioning without GPS measurements. Further work in the area of cellular network stability is presented in Chapter 4.

Positioning in synchronised networks, such as CDMA2000, is generally simpler than for unsynchronised network, since the transmitters are synchronised and a TDOA or TOA approach can be used. Caffery *et al.* (1998b) provide a comprehensive overview of the methods available for positioning in CDMA cellular networks. Positioning in CDMA2000 is the central topic of Chapter 5.

Early systems used Cell-ID to determine the mobile of the user terminal. The identity of the nearest base station is used as the position of the mobile. AOA is

generally available as well, since most cells are divided into sectors, with a different transmitter identity in each sector. Cell-ID and AOA methods demand some knowledge about the identity, coverage pattern, and positions of the BTSs. This information is generally not available, unless a company which develops the positioning technology has entered an agreement with the network's operator. Alternatively, the developer of a positioning method can perform a survey of the operator's network. The most cost-efficient method to do so is to exploit the user's handsets as measuring equipment, an approach which is possible only if the technology developer already has access to a large number of users.

Assisted-GNSS receivers

Most of the radio-positioning systems based on the signals from cellular base stations have difficulties reaching the requirements set by the FCC. These difficulties, combined with the increasing affordability of GNSS receiver chips and the demand for more accuracy from LBSs, have favoured the installation of GNSS receivers in cellular devices. The performance of these receivers can be improved by using external information accessible via the cellular data connection. The cellular network thus brings *assistance* information to the GNSS receiver. I explain the operation of an assisted-GNSS receiver in Section 2.5.

1.4 Thesis outline

Assisted-GNSS receivers have different architectures and operations from conventional receivers. The performance of conventional receivers has been investigated extensively in the existing literature, in both theoretical and experimental studies. However, the performance of assisted receivers has not received the same attention. Furthermore, the performance of an assisted receiver depends on the performance of the cellular network, which is generally not addressed in the literature.

The central topic of this thesis is the analysis of the performance of assisted-GPS receivers. I analysed the acquisition performance from a theoretical point of view and I evaluated the characteristics of the cellular networks through experiments. The plan of this thesis follows the chronology of my work. I first developed an analytical framework to evaluate the theoretical time-to-first-fix of assisted-GPS receivers, which is presented in Chapter 3. I regulated the theoretical model with experimental measurements in order to analyse the minimum bound of the time-to-first-fix in a real environment. I then focused on the quality of the assistance data provided by a real GSM cellular

network. I improved the stability of the timing signals and the results of this work are detailed in Chapter 4. Finally, I evaluated a method to position a handset in a CDMA2000 network. The results of these experiments are described in Chapter 5.

Estimation and detection in navigation receivers

The acquisition of a radio-frequency signal is one of the main topics of this thesis. We will encounter signals coming from GPS satellites and GSM and CDMA2000 base stations. These signals need to be received and decoded, operations which are better understood in terms of *parameter estimation* and *signal detection*. These concepts have been studied in several textbooks and I focus on the aspects relevant to this thesis. The theoretical foundations are treated in great detail by Van Trees (1968) and Kay (1993), while Pany (2010) provides more information about the application of these principles to GNSS receivers.

I introduce some theoretical principles of signal estimation and detection, then I apply these results to the case of pseudo-noise signals. Pseudo-noise signals are used in most GNSS constellations and in the CDMA2000 cellular network that is the subject of Chapter 5. We also review the estimation problem in dynamic linear systems and we introduce the Kalman filter. The work presented in this thesis is focused on the performance of assisted receivers and I discuss the architecture and operations of this type of receivers at the end of this chapter.

Estimation theory generally belongs to either one of two different branches of probability theory: the *Bayesian* approach or the *frequentist* approach. The Bayesian approach is generally preferred as it avoids many of the pitfalls found in frequentist methods, as discussed in detail in Jaynes (2003). However, the frequentist approach is commonly encountered in signal processing, as it is easier to implement and does not bring a significant degradation of the results when compared with the Bayesian

approach. I used maximum-likelihood methods, which are frequentist, to estimate the parameters of digital signals such as the baseband signal of a radio receiver. Bayesian methods were reserved for the processing of higher-level data, such as the receiver position estimates or the time deviations of an oscillator.

2.1 Parameter estimation

We seek to estimate the unknown values of the parameters of a probabilistic model representative of a real system. Observation of the physical system gives measurements, from which we can infer the values of the model parameters. Parameter estimation is not concerned about whether the observations are compatible with the model or whether another model could explain the observations better. This task will be performed in the detection stage, which we study in Section 2.2.

We first introduce some general concepts about estimation and probability theory. We then address the general problem of estimating the parameters of a signal in noise and we study in more detail the case of pseudo-noise signals. Finally, we look at the estimation of parameters in the case of a dynamic linear model and introduce the linear Kalman filter. This method will be used in Chapters 4 and 5, when filtering the timing measurements from cellular base stations.

Maximum-likelihood estimation

The estimation process produces information about the plausible values of the vector of parameters, θ , of the model under consideration. The system is observed and the measurement are denoted \mathcal{D} . All the knowledge about the probabilistic model is enclosed in the likelihood function, $p(\mathcal{D}|\theta)$, which describes the relationships between the model, the parameter vector, θ , and the observations, \mathcal{D} . The parameter vector is the variable of the likelihood function and the observation vector, \mathcal{D} , is a constant. It is often convenient to rewrite the likelihood function as

$$\mathcal{L}(\theta|\mathcal{D}) = p(\mathcal{D}|\theta),$$

which highlights the dependence of the parameter vector and the fact that the likelihood function is *not* a probability density function.

How the inference about the parameters is performed depends on the approach to probabilities one takes. The frequentist approach treats the parameters as unknown, yet non-random, variables. Estimation using frequentist methods gives a single point

estimate of the parameter, called the *maximum-likelihood* (ML) estimate, which is defined as

$$\hat{\theta} = \arg \max_{\theta} \mathcal{L}(\theta|\mathcal{D}).$$

Bayesian methods, on the other hand, treat the parameters as random variables with known prior probability distributions. The result of the inference is contained in the *posterior* distribution of the parameters. The Bayes theorem gives the relationship between the prior distribution, of probability density function $p(\theta)$, and the posterior distribution, $p(\theta|\mathcal{D})$, as

$$p(\theta|\mathcal{D}) = \frac{1}{K} \mathcal{L}(\theta|\mathcal{D}) p(\theta),$$

where K is a normalising constant, also called evidence or marginal likelihood. More formally, $K = \int_{\theta} \mathcal{L}(\theta|\mathcal{D}) p(\theta) d\theta$.

Bayesian inference thus does not produce a single point estimate of the parameter values. The information is contained in the entire posterior distribution. However, we often need a point estimate in order to make decisions. Berger (1985) discusses how the loss functions, which can be subjective and depends on the decision problem, affect the function used to generate the point estimate. This discussion is not necessary for this thesis, yet it provides some useful insight about the meaning of statistical estimators. The main points are that the maximum-a-posteriori (MAP) estimate, $\hat{\theta}_{\text{MAP}} = \arg \max_{\theta} p(\theta|\mathcal{D})$, corresponds to the maximum-likelihood estimate with a uniform prior distribution; the posterior mean corresponds to a quadratic loss function; and the posterior median corresponds to a linear loss function.

General signal in noise

We first review the maximum-likelihood estimation of parameters with a particular emphasis on radio signals. For now, we consider a general complex signal $x(t, \theta)$ where θ is the parameter vector of interest and t is the time. This signal is transmitted over an additive white Gaussian noise (AWGN) channel.

This representation is typical of the *equivalent baseband signal* in a radio-frequency receiver. Proakis (2000), among others, reviews the differences between passband and baseband representations. The Gaussian noise introduced by the channel is represented at baseband by a Gaussian random process $v(t)$ whose covariance function has the following properties: $\langle v(t) v^*(t') \rangle = N_0 \delta(t - t')$, where δ is the Dirac function and N_0 is the dual-sided noise power spectral density. The received signal, $z(t)$, is thus $z(t) = x(t, \theta) + v(t)$.

The continuous-time baseband signal is then sampled and converted to a discrete signal. The sampling period is T_s and the sampling frequency, f_s , is $f_s = 1/T_s$. The sampling instants, t_k , are thus $t_k = kT_s$. M samples of the received signals are represented by the vector $\mathbf{z}_{1:M} = [z_1, \dots, z_M]$, with

$$z_k = x(t_k, \boldsymbol{\theta}) + v_k,$$

and v_k is a sequence of independent, complex, Gaussian random variables. The sequence v_k represents the noise after sampling. The mathematical representation of a stochastic process, such as the noise process $v(t)$, after the sampling operation requires some attention. The statistical properties of the complex noise sequence v_k are now $\langle v_k v_{k'} \rangle = \sigma^2 \delta_{k-k'}$, with δ_k is the Kronecker delta function. The noise variance is $\sigma^2 = N_0 f_s$ and we neglect the quantisation noise.

The likelihood function of the parameter vector $\boldsymbol{\theta}$ in the presence of a signal and given the observed signal $\mathbf{z}_{1:M}$ is

$$\mathcal{L}(\boldsymbol{\theta}|\mathbf{z}_{1:M}) = p(\mathbf{z}_{1:M}|\boldsymbol{\theta}) = \frac{1}{(\pi\sigma)^M} e^{-\frac{1}{\sigma^2} \sum_{k=1}^M |z_k - x(t_k, \boldsymbol{\theta})|^2}. \quad (2.1)$$

The logarithm of the likelihood function, or log-likelihood, is more commonly used.

$$\begin{aligned} \log \mathcal{L}(\boldsymbol{\theta}|\mathbf{z}_{1:M}) &= -\frac{1}{\sigma^2} \sum_{k=1}^M |z_k - x(t_k, \boldsymbol{\theta})|^2 + K \\ &= -\frac{1}{\sigma^2} \sum_{k=1}^M \left[|z_k|^2 + |x(t_k, \boldsymbol{\theta})|^2 - 2 \operatorname{Re} \left(x(t_k, \boldsymbol{\theta}) z_k^* \right) \right] + K, \end{aligned}$$

where $K = -N/2 \log(\pi \sigma^2)$.

This relationship can be understood by introducing the energies, divided by the sampling period, contained in a signal of length M samples. The energy of the signal of interest is $E_x(\boldsymbol{\theta}) = \sum_{k=1}^M |x(t_k, \boldsymbol{\theta})|^2$ and the energy contained in the received signal, $\mathbf{z}_{1:M}$, is $E_z = \sum_{k=1}^M |z_k|^2$. The log-likelihood can then be written as

$$\log \mathcal{L}(\boldsymbol{\theta}|\mathbf{z}_{1:M}) = K - \frac{E_x(\boldsymbol{\theta}) + E_z}{\sigma^2} + \frac{2}{\sigma^2} \operatorname{Re} \left(\sum_{k=1}^M x(t_k, \boldsymbol{\theta}) z_{1:M}^* \right). \quad (2.2)$$

The log-likelihood can be interpreted geometrically: if we consider the vectors containing the theoretical signal response $\mathbf{x}(\boldsymbol{\theta}) = [x_1(\boldsymbol{\theta}), \dots, x_M(\boldsymbol{\theta})]$ and the vector of observations $\mathbf{z}_{1:M}$, then we can express the log-likelihood in term of the dot product of the two vectors: $\log \mathcal{L}(\boldsymbol{\theta}|\mathbf{z}_{1:M}) = 2 \operatorname{Re} (\mathbf{x}(\boldsymbol{\theta}) \cdot \mathbf{z}^*)$. The algebraic representation leads to a geometric interpretation: the maximum of the likelihood is reached when the parameters are adjusted so that the vector of the received measurements is parallel to the vector formed by the samples of the theoretical signal sent.

Estimation of pseudo-noise signals

The signal model is now set to represent a pseudo-noise signal, typical of a direct-sequence spread-spectrum signal used by GNSSs. The continuous-time signal of interest has the form

$$x(t, a, \tau, f) = a g(t - \tau) e^{j2\pi f t}, \quad (2.3)$$

where a is the complex amplitude of the baseband signal, $g(t)$ is the spreading code sequence, τ is the code-phase delay and f is the residual frequency in the baseband signal. The residual phase offset is included in the complex amplitude a . The power of the signal modelled by Equation 2.3 is constant and, therefore, $E_x(\theta) = N|a|^2$. One should remember that this is the power of the baseband signal – the power of the signal-in-space of the GNSS satellites, C , which is reported in the ICD, is generally given for the RF carrier signal, which is half the power of the baseband signal, $C = \frac{|a|^2}{2}$. The log-likelihood function of the baseband signal can be derived from Equation 2.2 and written as

$$\log \mathcal{L}(\theta | \mathbf{z}_{1:M}) = K - \frac{N|a|^2 + E_z}{\sigma^2} + \frac{2}{\sigma^2} \operatorname{Re} \left(\sum_{k=1}^M a g(t_k - \tau) e^{j2\pi f t_k} z_k^* \right). \quad (2.4)$$

The parameters of interest are now $\theta = (a, \tau, f)$. In a GNSS receiver, τ is related to the pseudo-range and f to the frequency offset, which is caused by the Doppler effect and the frequency bias of the local oscillator. These two parameters are often called the *synchronisation parameters* in the spread-spectrum communication literature. The amplitude, a , is generally treated as a *nuisance* parameter, which we do not seek to estimate explicitly. Pany (2010), among others, shows that the maximum-likelihood estimate of the amplitude, \hat{a} , can be calculated as

$$\hat{a}(\tau, f) = \frac{1}{N} \sum_{i=1}^M z_i g^*(t_i - \tau) e^{-j2\pi f t_i}. \quad (2.5)$$

We can then replace the amplitude a by its estimate \hat{a} in the likelihood function, a substitution that does not affect the results because of the invariance principle applied to maximum-likelihood estimation. The expression also highlights the importance of the *correlators* to detect and estimate the signal parameters. A correlator of length M performs the operation

$$S_n(\tau, f) = \sum_{k=n}^{n+M+1} z_k g^*(t_k - \tau) e^{-j2\pi f t_k}, \quad (2.6)$$

where n is the index of the first sample of the signal to be correlated. The correlator is, intuitively, an operation that matches the received signal with the conjugate of the

theoretical signal. This operation is also called *matched filtering*. The matched filter is commonly found in the signal estimation literature, in particular for the processing of Radar signals. The matched filter can also be derived directly by calculating the filter that maximises the signal-to-noise ratio at the receiver. The derivation I presented here highlights the fact that the amplitude parameter is treated as a nuisance parameter, and that better knowledge about the distribution of the signal strength may lead to a different estimator.

The log-likelihood function of the general estimation problem, given in Equation 2.2, can now be written as

$$\begin{aligned} \log \mathcal{L}(\tau, f | \mathbf{z}_{1:M}) &= K - \frac{M|\hat{a}(\tau, f)|^2 + E_z}{\sigma^2} + \frac{2}{\sigma^2} \operatorname{Re} [M \hat{a}(\tau, f) \hat{a}^*(\tau, f)] \\ &= \frac{|S_1(\tau, f)|^2 - E_z}{\sigma^2} + K. \end{aligned} \quad (2.7)$$

The goal of a navigation receiver is to estimate the pseudo-range, calculated from the code-phase estimates $\hat{\tau}$, of each transmitted signal in order to calculate the position. The residual frequency, \hat{f} , is also desired for reasons that will be explained in Chapter 3. The maximum-likelihood estimates of the synchronisation parameters, $\hat{\tau}$ and \hat{f} , are obtained by maximising the likelihood function presented in Equation 2.7. Both these parameters only appear in $S_1(\tau, f)$, hence the entire estimation process only requires the output of the correlators, and the maximum-likelihood synchronisation parameters are

$$\hat{\tau}, \hat{f} = \arg \max_{\tau, f} |S_1(\tau, f)|.$$

We do not explain how the maximisation is performed at this stage, since it is usually performed at the same time as signal detection in a GNSS receiver. This point will be treated in more detail in Section 2.3.

We can also express the complex amplitude parameter as a combination of signal magnitude and residual phase. The magnitude is generally dealt with in the same way as we estimate the complex amplitude, using a maximum-likelihood estimate. However, the phase can be treated using a Bayesian approach, as proposed by Kay (1993). A common solution is to consider a uniform prior distribution for the phase, which leads to a closed-form expression of the likelihood function. However, the posterior distribution of the parameters can not, in general, be expressed as a closed-form expression. Pany (2010) notes that the Bayesian approaches used to estimate the synchronisation parameters of a GNSS receiver do not bring a significant advantage over maximum-likelihood methods.

Theoretical bounds of the code-phase estimator

The Cramér-Rao lower bound (CRLB) is a lower limit on the variance of an estimator of a non-random parameter. It is commonly encountered when comparing the performance of estimators based on the maximum-likelihood approach. The CRLB is a lower limit, which is not strictly *the* lowest limit in the general case. It is often possible to derive “tighter” limits to the performance of an estimator than the CRLB. The posterior Cramér-Rao bound is the Bayesian equivalent of the CRLB and it can be used to analyse the performance of single-point Bayesian estimate. I only used the frequentist definition of the CRLB.

The code phase is used to calculate the pseudo-range, which is then used in the position equation to determine the user position. Hence, the CRLB of the code-phase estimator is an important measure of the performance of a navigation system. Pany (2010) recalls that the CRLB of a code-phase estimator based on the correlation method is

$$\text{Var}(\hat{\tau}) \geq -\frac{1}{MT_s R''_{c,c^*}(0)C/N_0},$$

where $R''_{c,c^*}(t)$ is the second derivative of the autocorrelation function of the spreading code, and C/N_0 is the carrier-to-noise ratio, with C the carrier power and N_0 the noise power density. Intuitively, the function $R''_{c,c^*}(t)$ contains information about the “sharpness” of the peak of the autocorrelation function and thus the bandwidth of the navigation signal.

Similarly, Dardari *et al.* (2009) cite Kay (1993) and give the CRLB of the code-phase estimator

$$\text{Var}(\hat{\tau}) \geq \frac{1}{8MT_s \pi^2 \beta^2 C/N_0}, \quad (2.8)$$

where β is the effective channel bandwidth and is directly related to the channel frequency response, $P(f)$, by

$$\beta^2 = \frac{\int_{-\infty}^{+\infty} f^2 |P(f)|^2 df}{\int_{-\infty}^{+\infty} |P(f)|^2 df}.$$

Finally, the approach of Weiss *et al.* (1983) is not often quoted in the literature, although they propose tighter bounds of the time-delay estimator using a matched filter. They derive four different bounds, using the Ziv-Zakai method (Ziv *et al.*, 1969), which are valid over four intervals of the signal-to-noise ratio. They show that, for signals weaker than a calculated threshold, the code phase can not be recovered and the estimator is only bounded by the possible parameter space. They also show that the Ziv-Zakai bound at high signal-to-noise ratios coincides with the Cramér-Rao bound.

The CRLB is calculated for a simple propagation model, the additive white Gaussian noise channel without multipath propagation, in all the publications I have found.

We can learn two important points about the CRLB of the code-phase estimator from these equations. The CRLB becomes smaller, and thus the theoretical performance of the estimator improves, as the signal strength increases and the signal bandwidth becomes wider. Wider bandwidths are also privileged in practical applications as this facilitates multipath mitigation. Intuitively, it is easier for a radio-positioning system to identify the propagation conditions, and in particular the existence of multiple paths, when dealing with short pulses. A short pulse over a multipath channel is still visible if the delays between the paths are longer than the duration of the pulse. Algorithms can then identify the channel propagation conditions and use this information to mitigate the effects of multipath propagation. This possibility is a part of the rationale for ultra-wideband systems, which try to achieve the widest possible bandwidth to improve the position accuracy in challenging environments.

Estimation in dynamic linear systems

I now address the estimation of parameters in dynamic linear systems. This class of problems has been studied extensively, in particular since the introduction of the Kalman filter (Kalman, 1960). I recall only the main operations in a linear Kalman filter and more information can be found in Brown *et al.* (1997), for example.

The state of the dynamic system at time step k is represented by its state vector, \mathbf{x}_k . The observations, or measurements, \mathbf{z}_k are related to the state vector by the measurement function, expressed as a matrix H_k . The linear Kalman filter assumes that the measurements function is a linear function and the noise is additive white Gaussian noise. The *measurement equation* is

$$\mathbf{z}_k = H_k \mathbf{x}_k + R_k \mathbf{v},$$

where R_k is the covariance matrix of the observation noise and \mathbf{v} is a vector of independent normal random variables.

The state vector evolves over time according to linear dynamics, represented by the transition matrix F_k . This evolution is affected by the *process noise*, which is modelled as an additive white Gaussian noise. The process noise represents the noise introduced during the evolution of the system and, more generally, the uncertainty about the model. The *process model* is given by the linear equation

$$\mathbf{x}_k = F_k \mathbf{x}_{k-1} + Q_k \boldsymbol{\xi},$$

where Q_k is the covariance matrix of the process noise and ξ is a vector of independent normal random variables.

We now briefly introduce the two main steps of the Kalman filter. More information, including the *prediction* and the *update* equations, is provided in Brown *et al.* (1997). The Kalman filter equations provide an estimate of the state vector, represented as a Gaussian random variable. At the time step $k - 1$, the prior state is represented by the probability distribution $p(\mathbf{x}_k|\mathbf{x}_{k-1})$, which is a Gaussian distribution of mean $\hat{\mathbf{x}}_{k|k-1}$ and covariance matrix $P_{k|k-1}$. A measurement, \mathbf{z}_k , is then taken at time step k and the update equation is used to calculate the distribution of the posterior state, $p(\mathbf{x}_k|\mathbf{z}_k)$. The state is now represented by a Gaussian random variable of mean $\hat{\mathbf{x}}_{k|k}$ and covariance matrix $P_{k|k}$. The prediction equation is then applied to the posterior estimate in order to obtain the prior distribution at the next time step, $p(\mathbf{x}_{k+1}|\mathbf{x}_k)$. The Kalman filter thus alternates between the prediction and update equation in order to maintain an estimate of the state vector.

I now introduce the innovation vector and the log-likelihood function of a linear dynamic model, two notions that will be used in Chapter 4. The innovation, ϵ_k , is defined as

$$\epsilon_k = \mathbf{z}_k - H_k \hat{\mathbf{x}}_{k|k-1},$$

and the innovation covariance is

$$\Sigma_k = H_k P_{k|k-1} H_k^* + R_k.$$

The normalised innovation squared (NIS), e_k , is defined as

$$e_k = \epsilon_k \Sigma_k^{-1} \epsilon_k^T. \quad (2.9)$$

The normalised innovation squared is a useful measure of the goodness of fit of the model to the observations. It can be shown that, under the noise and dynamics assumption of the model, e_k follows a χ^2 distribution with d degrees of freedom, where d is the dimension of the state vector. The NIS is also used to calculate the log-likelihood function of the linear dynamic model. The logarithm of the likelihood function, $\mathcal{L}(\hat{\mathbf{x}}_k|\mathbf{z}_{1:M})$, is

$$\log \mathcal{L}(\hat{\mathbf{x}}_k|\mathbf{z}_{1:M}) = -\frac{1}{2} \sum_{k=1}^M e_k - \frac{1}{2} \sum_{k=1}^M \log |\Sigma_k| - \frac{Nd}{2} \log(2\pi). \quad (2.10)$$

Ristic *et al.* (2004), among others, shows how to calculate the CRLB of the state vector estimate.

2.2 Signal detection

We now seek to decide whether a signal is present among noisy observations. This problem is similar to hypothesis testing: either the observations contain both the signal and the noise, or they contain only the noise. The standard hypothesis testing problem assumes that the true parameters of the signals are known, under both hypotheses. We do not have such a knowledge with navigation signals. The code phase and the frequency residual parameters, for example, are not known since they are dependent on the user's position, which is what we want to estimate in the first place. The hypothesis testing problem with uncertain parameters is called a *composite* hypothesis problem. I first recall composite hypothesis testing and I discuss the case of pseudo-noise signals.

Composite hypothesis testing

A binary hypothesis test is composed of two hypotheses, H_0 and H_1 . Each hypothesis is associated with a probabilistic model, which is described by its likelihood function. We note $\mathcal{L}(H_0|x)$ and $\mathcal{L}(H_1|x)$ the likelihood functions of the model under the H_0 and H_1 hypotheses, respectively. It can be shown that the optimal test is based on the ratio of the likelihood (see, for example, Van Trees, 1968). This leads to the likelihood-ratio test (LRT), which is

$$\frac{\mathcal{L}(H_1|x)}{\mathcal{L}(H_0|x)} \gtrless \eta, \quad (2.11)$$

where η is fixed value called the *detection* threshold. The test decides for the H_1 hypothesis if the likelihood ratio test is greater than η , and for the H_0 hypothesis otherwise.

How the threshold, η , is chosen depends on the detection *criterion* that is used. There are two common criteria to choose the threshold from: the Bayes criterion and the Neyman-Pearson criterion. The Bayes criterion relies on decision theory; it requires that the prior probabilities of the hypotheses and the costs of making the wrong decisions are known. The Neyman-Pearson criterion does not require such information and the performance of the criterion is expressed in terms of *probability of false-alarm* and *probability of detection*. The probability of false alarm is the probability of deciding H_1 whereas H_0 is true, and the probability of detection is the probability of correctly detecting H_1 . The Neyman-Pearson criterion is more common than the Bayes criterion in signal analysis, since the prior probabilities of the hypotheses are generally not known. Berger (1985) provides an analysis of the foundations of decision theory when applied to statistical problems. For now, I assume that the threshold η is known, without specifying how it is calculated.

Equation 2.11 assumes that the likelihood functions does not depend on any parameter. The *generalised likelihood-ratio test* (GLRT) is often used when the likelihood functions do depend on parameters, like in composite hypothesis problems. The GLRT is similar to the likelihood ratio when both likelihood functions are set to their maximum-likelihood values. Formally, the generalised likelihood ratio is

$$\Lambda(x) = \frac{\max_{\theta \in \Theta|H_1} \mathcal{L}(\theta|x)}{\max_{\eta \in \Theta|x} \mathcal{L}(\eta|x)},$$

and the GLRT is

$$\Lambda(x) \lessgtr \eta.$$

Detection of pseudo-noise signals

We now use the generalised likelihood-ratio test to detect a pseudo-noise signal of unknown parameters in additive white Gaussian noise. The hypothesis H_1 is the hypothesis that the observations contain both signal and noise, whereas the hypothesis H_0 , called the *null hypothesis*, is the hypothesis that only noise is present. The likelihood function under the H_1 hypothesis is presented in Equation 2.7. The likelihood function under the null hypothesis is the same as Equation 2.7, with the amplitude parameter a set to zero. We assumed the noise variance is known and constant, hence $E_z(\theta)$ does not depend on any parameter. The log-likelihood functions under the H_0 and H_1 hypotheses are, respectively,

$$\log \mathcal{L}(\theta, H_0 | \mathbf{z}_{1:M}) = K - \frac{E_z}{\sigma^2}.$$

and

$$\log \mathcal{L}(\theta, H_1 | \mathbf{z}_{1:M}) = K + \frac{|S_1(\tau, f)|^2 - E_z}{\sigma^2}.$$

The GLRT can be expressed using the log-likelihood functions, which gives

$$\begin{aligned} \log \Lambda(\mathbf{z}_{1:M}) &= \log \mathcal{L}(\hat{\theta}, H_1 | \mathbf{z}_{1:M}) - \log \mathcal{L}(\hat{\theta}, H_0 | \mathbf{z}_{1:M}) \\ &= \frac{|S_1(\hat{\tau}, \hat{f})|^2}{\sigma^2}. \end{aligned} \tag{2.12}$$

The GLRT equation, described by Equation 2.12, only depends on the correlator value and the noise variance. This shows that the output of the correlator, $S_1(\tau, f)$, is the only variable needed both for the estimation and the detection step. These two steps are generally combined to form the *acquisition* step.

2.3 Acquisition of GNSS signals

The goal of the acquisition of a pseudo-noise signal is to estimate the values of the synchronisation parameters as well as to detect whether a signal is present at the receiver. It is thus a combination of the estimation and detection steps. The existing literature often introduces the acquisition process as an operation of its own, however it may be useful to remember the dual nature of the acquisition process.

Finding the synchronisation parameters

The generalised likelihood-ratio test, shown in Equation 2.12, is commonly used for the acquisition of GNSS signals. It only depends on the value of the correlator output, $|S_1(\hat{\tau}, \hat{f})|^2$, which is commonly called the *decision variable*. We first notice that maximising the likelihood function of the H_1 hypothesis, $\mathcal{L}(\hat{\theta}, H_1 | \mathbf{z}_{1:M})$, is similar to maximising the decision variable of the GLRT. This observation explains why it is easier to perform both the estimation and the detection in a single step.

So far, we have not discussed how the maximum-likelihood estimates of the frequency residual and code phase are found. As seen in Section 1.2, the PN code sequence of a GNSS signal is designed such that the value of its autocorrelation function is negligible everywhere except near the time origin. The likelihood function has thus a “sharp” peak around the correct values of the synchronisation parameters, but is relatively constant elsewhere, as shown in Figure 1.2. The only way to find the maximum is thus to calculate the likelihood function for all the possible values of the parameters. This method is in contrast to standard numerical optimisation methods, which generally use the derivatives of the likelihood function in order to find the maximum. The likelihood function of PN signals is constant almost everywhere, hence calculating the derivatives does not help focus the search for the maximum. The set of all the possible synchronisation parameters for which the likelihood function is calculated is called the *search space*. I discuss how the search space is built in Section 2.5.

Figure 2.1 is an illustration of the GLRT applied to the GPS L1 C/A signal. The figure shows that the correlator output, which is proportional to the log-likelihood function, has a clear peak around the maximum-likelihood parameters. The function is negligible elsewhere. The figure also illustrates the effect of the signal bandwidth on the accuracy of the code-phase estimate, as discussed in Section 2.1. The likelihood function around the peak is “smoother” for signals with narrower bandwidths, hence the degradation by the Gaussian noise is relatively more important than for a noise with same variance but added to a likelihood function with a “sharper” peak.

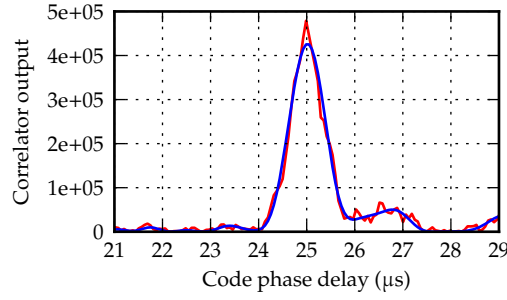


Figure 2.1: Illustration of the correlator output for different code-phases. The signal was generated with a true code-phase delay of 25 μs . The signal was representative of a GPS L1 C/A complex baseband signal of carrier-to-noise density ratio 42 dB–Hz and sampled at 10 MHz. The red curve represents the correlation value without any filtering, i.e. the bandwidth is limited by the Nyquist frequency. The blue curve shows the results after a low-pass filter of bandwidth 1 MHz.

Implementation of the detector

We now turn our attention to the decision variable, $|S_1(\tau, f)|^2$. The decision variable is the squared magnitude of the correlator output. The correlator integrates the incoming signal with the conjugate of a local replica. The introduction of the magnitude operator removes the phase mismatch between the received signal and its replica. The phase removal is also apparent when comparing the log-likelihood from Equation 2.4, before the complex amplitude parameter is estimated: only the real part of the correlator output is involved; the magnitude operation is introduced after the residual phase is estimated in Equation 2.5. The correlator is thus said to perform a *coherent* integration, which implies that the phase difference between the received signal, z_k , and its replica, $g^*(t_k - \hat{\tau})e^{-j2\pi\hat{f}t_k}$, does not change.

The *coherent integration* time, $T_{\text{coh}} = MT_s$, determines the sensitivity of a receiver, as shown by Equation 2.15. Intuitively, the longer the coherent integration time, the more sensitive the receiver is. It is, however, not always possible to extend the coherent integration indefinitely: any change in the amplitude, frequency or code phase of received signal during the coherent integration will degrade the performance of the detector. This can be understood by taking the example of the GPS navigation message. The navigation message is encoded by a binary phase shifting key modulation, where the data bits introduce a phase shift of 180° . If the coherent integration is performed during a bit transition, the integration of the signal after the bit transition cancels the accumulation before the transition. Similarly, the stability of the local oscillator may introduce frequency variations and the user motion may affect the signal code phases.

We can extend the concept of coherent integration to the decision variable. The sensitivity of the receiver can be improved by *non-coherent integration*. The non-coherent detector accumulates the correlator output for K_{nc} non-coherent integrations. This integration results in the non-coherent detector $Y(\tau, f)$, which is formally defined as

$$Y(\tau, f) = \frac{1}{K_{nc} M \sigma_z^2} \sum_{k=0}^{K_{nc}-1} |S_{(kM+1)}(\tau, f)|^2. \quad (2.13)$$

$Y(\tau, f)$ is now the decision variable of the GLRT detector. The noise variance is normalised to one by the coefficient before the summation in Equation 2.13. This normalisation is not required but it facilitates the expression of the probabilities of detection and false alarm. The acquisition process thus consists of finding the synchronisation parameters that maximise $Y(\tau, f)$,

$$\hat{\tau}, \hat{f} = \arg \max_{\tau, f} Y(\tau, f).$$

The decision rule is now

$$Y(\hat{\tau}, \hat{f}) \leq \eta,$$

where η is the decision threshold, calculated for the non-coherent detector. Pany (2010) offers a more complete discussion about how the non-coherent detector relates to the maximum-likelihood estimation of parameters when the received signal has a variable phase.

The GLRT detector needs to calculate the output of the non-coherent detector for all the possible values of the τ and f parameters in the search space. This two-dimensional search can be optimised so that all the values of correlators are calculated in one operation along the code-phase dimension. We want to calculate the output of the non-coherent detector, $Y(\tau, f_0)$ for a discrete set of M candidate code phases, $\tau_m = m\Delta\tau$ regularly spaced over the search space, at a fixed frequency offset f_0 . This requires M evaluation of Equation 2.6,

$$S_1(\tau_m, f_0) = \sum_{k=0}^M z_k g^*(t_k - m\Delta\tau) e^{-j2\pi f_0 t_k}. \quad (2.14)$$

The function shown in Equation 2.14, when considered for the variable m , is a discrete circular convolution, which can be calculated efficiently using a discrete Fourier transform. A software receiver can exploit this property to calculate efficiently the M correlator outputs using a fast Fourier transform (FFT), as explained by Davenport (1991).

Theoretical performance

The theoretical performance of the non-coherent detector can be measured in terms of detection and false-alarm probabilities. Let us consider a signal received with a carrier power C and a noise power spectral density N_0 . The carrier-to-noise-density ratio, C/N_0 , is often used to evaluate the performance of a detector as a function of the signal strength. The receiver is similar to the non-coherent detector described in Equation 2.13, using a detection threshold η , a coherent integration time T_{coh} , and K_{nc} non-coherent integrations. The probability of detection is

$$p_d = Q_{K_{\text{nc}}}(\sqrt{\lambda}, \sqrt{\eta}), \quad (2.15)$$

with $\lambda = 2K_{\text{nc}}T_{\text{coh}}C/N_0$ and $Q(a, b)$ is the Marcum Q-function. λ is sometimes called the post-integration signal-to-noise ratio. The probability of false alarm is

$$p_{\text{fa}} = 1 - \tilde{\Gamma}_{K_{\text{nc}}}(\eta/2), \quad (2.16)$$

where $\tilde{\Gamma}_k(x)$ is the regularised Gamma function. The Marcum Q-function and the regularised Gamma function are commonly found in scientific software packages.

These two probabilities are used in the Neyman-Pearson criterion in order to choose the detection threshold, η . There is a trade-off between these two probabilities: the probability of false-alarm and of detection both increase as the threshold gets lower. However, the goal is to obtain a high probability of detection and a low false-alarm rate. This goal can be achieved by either increasing the integration length, reducing the noise figure of the receiver, or, if practical, improving the signal strength.

Tracking of synchronisation parameters

It is common to *track* the synchronisation parameters once their initial values have been calculated, without having to restart the entire acquisition process. The tracking is generally performed by a phase-locked loop for the residual frequency and by a delay-locked loop for the code phase. The theoretical analysis and the practical implementation of tracking have been extensively studied; a reference, among others, is Parkinson *et al.* (1996), who investigate the design of tracking loops for GPS receivers. Most of the work presented in this thesis is focussed on assisted receivers, which do not require tracking loops. I implemented tracking loops in my software GNSS receiver in order to decode the navigation message. Nevertheless, we do not need any theoretical background about tracking loops for the work presented in this thesis.

2.4 Position estimation

One of the final tasks of a GNSS receiver is to calculate the position by solving the *position equation*, presented in Section 1.1. We only consider the TOA position equation in this thesis, although the TDOA equation can be solved with a similar method. In practice, Ju-Yong Do *et al.* (2007) have shown that the TOA approach leads to more robustness when the statistics of the measurement noise are not fully known.

We now extend the position equation, Equation 1.1, for the case of pseudo-noise signals. The code phases, τ_i , of the pseudo-noise signals transmitted from satellite number i , are directly related to the pseudo-range, ρ_i . The difference between the two comes from the uncertainty introduced by the repetition period, T_{CA} , of the PN code of the GPS C/A code. The pseudo-ranges are calculated by decoding the navigation message and identifying a pattern of navigation bits that is common to all the signals. In practice, the time-of-week field is almost always used as it is also required to calculate the satellite positions at the time of transmission. However, other patterns can be used if the positions of the satellites are already known. The number of full code periods, N_{TOW} is then counted from this field and added to the code phase to form the pseudo-range measurement ρ_i ,

$$\rho_i = c(\tau_i + N_{TOW}T_{CA}). \quad (2.17)$$

Solution to the position equation

We assume the code-phase estimation step previously described has calculated the pseudo-range estimates, $\hat{\rho}_i$, and the uncertainty is represented by additive white Gaussian measurement noise. The TOA position equation with N noisy pseudo-range measurements can thus be written

$$\hat{\rho}_i = \|\hat{\mathbf{x}} - \mathbf{x}_i\| - c\hat{b}_u + v_i,$$

where $\mathbf{v} = [v_1, \dots, v_N]$ is a multivariate Gaussian random vector of covariance matrix Σ_ρ , representing the measurement noise.

The position equation is non-linear and an approximate solution of the maximum-likelihood position estimate is usually found using the iterative least-squares algorithms, an approach which is found in early receivers (Parkinson *et al.*, 1996, chapter 9), modern software receivers (Borre *et al.*, 2007), and assisted receivers (van Diggelen, 2009). The basis of the method is to linearise the position equation around a coarse estimate, solve the equation using linear methods, and iterate with the new estimate. The first

derivatives, which are required to linearise the function, are

$$\mathbf{u}_i = \frac{\delta \rho_i}{\delta \mathbf{x}} = \frac{\hat{\mathbf{x}} - \mathbf{x}_i}{\|\mathbf{x} - \mathbf{x}_i\|}$$

and

$$\frac{\delta \rho_i}{\delta \hat{b}_u} = -c$$

\mathbf{u}_i is also the unit vector between the user position and the satellite i . The unit vectors are often used to form the *geometry matrix*, \mathbf{G} , commonly encountered in positioning problems. \mathbf{G} is defined as

$$\mathbf{G} = \begin{bmatrix} \mathbf{u}_0 & -c \\ \vdots & \vdots \\ \mathbf{u}_N & -c \end{bmatrix}$$

We introduce the augmented state vector, $\theta = [\mathbf{x}, \dots, b_u]$, which contains all the parameters we wish to estimate. The first-order linearisation of the position equation leads to the difference equation

$$\Delta \rho = \mathbf{G} \Delta \theta + \epsilon, \quad (2.18)$$

where ϵ is the approximation error and $\Delta \rho = [\Delta \rho_1, \dots, \Delta \rho_N]$ is the difference between the theoretical and observed pseudo-range vector.

The maximum-likelihood estimate, $\hat{\theta}$, is approximated by an iterative algorithm. An approximate position, generally the previously calculated position, is used as an initial value of the estimate, $\hat{\theta}^{(0)}$. The following algorithm is then iterated over k :

$$\begin{aligned} \Delta \rho_i^{(k)} &= \|\hat{\mathbf{x}}^{(k)} - \mathbf{x}_i\| - c \hat{b}_u^{(k)} \quad \text{for each } i \\ \Delta \theta^{(k)} &= (\mathbf{G}^t \Sigma_\rho^{-1} \mathbf{G})^{-1} \mathbf{G}^t \mathbf{R}^{-1} \Delta \rho^{(k)} \\ \hat{\theta}^{(k+1)} &= \hat{\theta}^{(k)} + \Delta \theta^{(k)} \end{aligned}$$

where $\hat{\mathbf{x}}^{(k)}$ and $\hat{b}_u^{(k)}$ are the estimates at iteration k , contained respectively in the first three components and the last component of $\hat{\theta}^{(k)}$.

The vector $\Delta \rho$ is called the vector of *pseudo-range residuals* and $\Delta \theta$ the vector of parameter residuals. The residuals are often used to check the behaviour of the algorithms. It can be shown, for example, that the distribution of the residuals follows a Gaussian distribution, under the AWGN noise assumptions.

There are different possible stopping rules for the iteration loop. A common choice is to stop when the sum of the squares of the residuals is below a given threshold. The position equation is generally a well-posed problem and the algorithm generally converges in less than ten iterations..

Dilution of precision

We can calculate the Cramér-Rao bound of the position estimate calculated by the iterative least-square algorithm. With Σ_ρ the measurement noise covariance matrix of the measurement noise and G the geometry matrix, the CRLB matrix is

$$\text{CRLB}^{-1} = G \Sigma_\rho^{-1} G^T. \quad (2.19)$$

The matrix Σ_ρ is generally not known accurately. The noise variances of the pseudo-range measurements can be estimated from Equation 2.8, which depends on the signal strengths. However, that equation is only a lower bound, and effects such as multipath propagation and the non-Gaussianity of the noise affect the exact noise variance. The cross-correlations between the pseudo-range measurements of the different satellites are generally unknown, although the propagation conditions around the user may introduce correlations. As a result, the measurement noise covariance, Σ_ρ , is generally unknown. It is often convenient to analyse the theoretical performance of a receiver based on the transmitter geometry alone. These effects are summarised in the *dilution of precision* (DOP) metric, which isolates the effects of the measurements noise by setting the noise covariance matrix to the identity matrix. The DOP matrix, DOP , is thus

$$\text{DOP} = G G^T. \quad (2.20)$$

Specific measures of the DOP are often encountered. The horizontal dilution of precision (HDOP) measures the effect of the geometry on the horizontal position only. It is equal to the trace of the horizontal components of the DOP matrix. Chaffee *et al.* (1994) give a more complete treatment of the theoretical limits of the position calculation.

Solution in the position domain

The iterative least-squares is the most common method to calculate the user position. Alternative methods have been proposed recently, which are based on the direct calculation on the maximum-likelihood estimate of the position, without the intermediate step of estimating the synchronisation parameters. Closas *et al.* (2007) recall the likelihood function in the position domain and propose a numerical approach to find its maximum. Axelrad *et al.* (2011) investigate the advantages of the direct positioning method with weak signals. An advantage of methods based on the likelihood function is that it combines the signals from all the satellites, even if the signal strengths of some individual satellites are too weak to be able to estimate the synchronisation parameters – the information contained in these weak signals is still included in the solution. One

of the problem faced with this method is the size of the search space, which is now composed of the three spatial dimensions plus the user bias. A good estimate of the user position, and possibly the user clock bias, is required in order to reduce the search space to a tractable size. The need for a fourth variable in the search, for the user bias, is not always explicitly mentioned in the literature. I considered the direct positioning approach in my work, in particular because the method could benefit significantly from an estimate of the user clock bias, however the results of my early investigations are not reported in this thesis.

2.5 Assisted-GNSS receivers

I now describe the operation of assisted-GNSS receivers, typically encountered in cellular devices. The literature about assisted receivers is not as large as the one about conventional receivers, despite the wide popularity of assisted receivers in consumer devices. An analysis of the architecture and the performance of these receivers is provided by van Diggelen (2009).

Description

An assisted-GNSS receiver is a type of receiver that uses external information, called *assistance data*, in order to improve the positioning and navigation performance. The assistance data generally consists of the approximate universal time and position of the receiver, as well as the ephemeris data of the GNSS constellation.

Tracking loops, which are used to decode the GPS navigation message, are generally absent in an assisted-GPS receiver since the navigation message is provided by the assistance data. However, decoding the TOW field from the navigation message is required in order to calculate the pseudo-range, as shown by Equation 2.17. The only information available to an assisted receiver in order to calculate the position is the code phase, which differs from the pseudo-range by an integer number of code periods. We can still calculate the user's position with only code phases, by using the position equation

$$\tau_i = \frac{1}{c} \|\mathbf{x}_i(\text{TOT}_i) - \mathbf{x}\| - b_u + n_i T_{\text{PN}}, \quad (2.21)$$

where n_i is the integer number of repetitions of the PN code since the time at which the signals have been transmitted and TOT_i is the unknown time of transmission of the signal coming from satellite i . The satellite positions, $\mathbf{x}_i(\text{TOT}_i)$, are now dependent on an unknown variable whereas a conventional receiver can calculate the satellite positions

from the known times of transmission of the signals. A conventional GPS L1 C/A receiver, for example, can decode the TOW field of the navigation message and calculate the satellite positions at that epoch, using the ephemeris carried in the navigation message. An assisted receiver, on the other hand, solves the position equation by adding TOT_i to the set of unknown variables, which now becomes (\mathbf{x}, b_u, TOT_i) . The integer number of code periods, n_i , is unknown but is not part of the set of unknown variables. It can be calculated directly if the approximate universal time and position of the receiver are known within some maximum error bounds. Similarly, TOT_i is constrained to be an integer number of code periods, hence all the times are known as soon as the TOT of a specific i has been calculated. These methods are often called *millisecond-ambiguity* positioning methods, in reference to the 1 ms code period of the C/A code. The measurements are now the *fractional* pseudo-range, cp_i , in contrast to the full pseudo-range measurements given in Equation 2.17.

Lannelongue *et al.* (1998) and van Diggelen (2009) show how the position can be calculated with a least-squares algorithm similar to the one presented in Section 2.4. There are now five unknown variables, thus requiring the pseudo-range measurements from at least five satellites in order to solve the position equation. Sirola *et al.* (2002) show how the position equation converges to the correct solution if the initial time and position are known within some error domain. The error domain that guarantees the convergence has a conical shape, which extends over the maximum time errors of ± 3.5 min and a diameter which is the maximum position error of 150 km for the GPS C/A code.

Assisted-GNSS receivers have multiple advantages that make them desirable in consumer devices. The absence of tracking loops simplifies the design of the receiver and reduces the physical size of the chip, which facilitates its integration on existing semiconductor chips. On the one hand, not needing to decode the navigation message has the drawback of requiring one more unknown variable than in a conventional GPS receiver. On the other hand, it has the advantage of allowing the operation of the receiver with weaker signals, since the signal strength required to decode the navigation message is generally higher than the signal strength required to estimate the pseudo-ranges. Furthermore, the time-to-first-fix (TTFF) is improved in assisted-GNSS receiver, using two mechanisms. The receiver does not need to decode the satellite ephemeris data, which can take up to 30 s using the GPS L1 C/A signal, since the ephemeris is contained in the assistance data. The millisecond-ambiguity positioning also improves the TTFF since the receiver does not have to identify and record the TOW field. For these reasons, some receiver manufacturers also use the term *snapshot*

or *push-to-fix* positioning to describe this approach.

Assistance data

The performance of an assisted receiver is dependent on the amount and quality of the assistance information available. We only consider the case of assistance data provided by a cellular communication networks, for example a GSM network. Assistance data is not always available and, when available, the level of information is contingent on the assistance technologies used by the cellular network operator. Position assistance is provided by cellular positioning technologies such as the ones reviewed in Section 1.3. The time assistance is dependent on the cellular network architecture. Unsynchronised networks, such as GSM networks, are generally less capable of providing accurate time information than are synchronised networks. The time accuracy achieved in a GSM network is the topic of Chapter 4.

Cellular transmitters usually employ high-quality oscillators to generate the radio-frequency carriers. The accuracy of the carrier frequency can be used to correct the frequency bias of the local oscillator of the receiver. This form of assistance is not directly explicitly provided by the cellular network to the acquisition engine of the GNSS receiver. Instead, it is implemented in the handset transceiver, which locks its local oscillator onto the radio-frequency carrier. The same local oscillator can be used by the GNSS receiver, hence the stability of the local oscillator is the same as the stability of the oscillators in the cellular BTSs. The apparent carrier frequency is affected by the Doppler effect caused by the velocity of the mobile device and by the frequency variations caused by multipath propagation. The stability of an oscillator locked onto the carrier frequency is therefore not necessarily as good as the stability of the BTS clocks. Furthermore, the frequency accuracy and stability provided by the cellular network does not guarantee the time accuracy or the phase stability of the GSM synchronisation signals, as the RF carrier and the cellular signals may be controlled by different oscillators.

There is no general agreement as to what typical levels of assistance should be considered and terms such as “coarse assistance” and “fine assistance” have different meanings for different authors. I consider three different scenarios all along this thesis, outlined in Table 2.1. The low-level scenario is typical of a mobile device without cellular connectivity. The time is provided by the internal clock, the position is taken as the previous calculated position, and the short-term ephemeris is not available. The medium-level scenario corresponds to a device operating in an unsynchronised network, for example a GSM network. Cell-ID is generally available, although its

position uncertainty is similar to the radius of a cell. The local oscillator is locked on the RF frequency, yet the timing signals of the unsynchronised network can not provide time accuracy better than a few seconds of the universal time. Finally, the high-level scenario is representative of a synchronised cellular network, which can provide the universal time with a good accuracy. The time uncertainty mainly comes from the uncertainty in the time of flight of the signal from the base station.

Table 2.1: Scenario assumptions.

Aiding scenario	Data network	Errors		Oscillator stability	Almanac	Ephemeris
		Position	Time			
Low level	No	≤ 300 km	≤ 5 min	1 ppm	Yes	No
Medium level	Yes	≤ 30 km	≤ 5 s	0.1 ppm	Yes	Yes
High level	Yes	≤ 30 km	≤ 10 μ s	0.1 ppm	Yes	Yes

Assisted receivers also differ in how the position is calculated. The synchronisation parameters are generally estimated by the mobile device, but the position calculation can be performed using either an MS-based or MS-assisted method. The position is calculated on the device in an MS-based method. On the other hand, an MS-assisted method consists of transmitting the synchronisation parameter estimates to a location server on the cellular network; the server calculates and then returns the position to the mobile station. The MS-assisted method has the advantage of simplifying the design of the mobile device and it may also exploit more information than is available on the device. The main drawback is the need for a data access to the cellular network. An even more decentralised method has been proposed in the literature, in which the baseband signal is simply transmitted to a server that calculates the position.

2.6 Summary

In this chapter, we have reviewed the bases of the acquisition of direct sequence-spread spectrum signals, which are often encountered in GNSS and cellular systems. I highlighted the distinction between parameter estimation and signal detection, although the acquisition process may also be understood using different approaches, such as by introducing the matched filter. I outlined the foundations of frequentist and Bayesian estimation. We looked at the estimation of the synchronisation parameters of pseudo-noise signals and the theoretical bound on the code-phase estimation. We also investigated the estimation of the user position by using an iterative least-squares algorithms and we introduced the dilution of precision as a theoretical bound of the

position error. Finally, we reviewed the operation and architecture of assisted-GNSS receivers. These results will be continuously used in the remainder of this thesis.

Analysis of the time-to-first-fix in assisted-GNSS receivers

The time-to-first-fix (TTFF) is a metric commonly used to evaluate the performance of a GNSS receiver. It is informally defined as the time taken by the receiver to calculate a position, also called a *fix*, from the instant the user has turned on the receiver. This metric is particularly important for location-based services on mass-market devices, such as smartphones, for which a quick position fix is often more valuable than an accurate position. Many applications can work with an approximate position; however the response time of the application, which is strongly dependent on the TTFF, must remain short to ensure a positive user experience.

Optimisation of the TTFF is a challenging problem to the GNSS receiver designer. The current options are either to run Monte-Carlo simulations with a theoretical receiver model or to repeat several acquisitions on a real receiver connected to a signal simulator. Both these techniques are time-consuming, which hinders the optimisation of the TTFF. An alternative approach is to develop an analytical model that can be analysed and optimised more easily. This approach has been under investigation since the introduction of spread-spectrum signals, with Holmes *et al.* (1977) and Hopkins (1977) presenting early studies.

Analytical methods have been limited to calculating statistics, such as the mean and the standard deviation, of the acquisition time of just one satellite. Extracting information about the TTFF from such descriptive statistics, the mean time to acquire *all* the satellites for example, cannot be calculated from the mean times of each acquisition individually. Extending these methods, which are valid for the acquisition of a single

satellite, to the case of multiple satellites is not straightforward. Additional information is needed, such as the probability distributions of the individual acquisition times. Typical GNSS receivers require at least 4 satellites in order to calculate a position, so that existing methods cannot be used directly to analyse the TTFF. It may also be desirable to calculate the performance at a specific confidence level, for example the 90% probability of the TTFF. This is not possible if the probability distribution is unknown.

In this chapter, I derive the theoretical distribution of the TTFF of an assisted-GNSS receiver. First, I review previous studies on the acquisition time of spread-spectrum signals and highlight some properties of probability generating functions (PGF). I then investigate the model of an assisted receiver and I discuss the assumptions made. I then calculate the probability distribution function of the TTFF using this model and results of previous studies. I illustrate the method with a simple scenario, and provide further analysis by using real measurements. Finally, I discuss the limitations and the opportunities for improving this new method.

An early version of this work was presented in Couronneau *et al.* (2011), where the acquisition of one signal only was considered. I extend that work in this chapter by modelling the two-stage acquisition process of an assisted receiver.

3.1 Analysis of the acquisition of direct-sequence spread spectrum signals

The theoretical acquisition time of pseudo-noise signals has been investigated since the introduction of spread-spectrum systems and CDMA communications. Different techniques have been proposed and, in this chapter, we will focus on the most general method and its application to GNSS receivers.

Signal acquisition model

The goal of the acquisition process is to find the most likely set of *synchronisation parameters* of the signal. In spread-spectrum communications, the synchronisation parameters are the parameters that a receiver needs in order to decode the received signal. The synchronisation parameters for the signal transmitted from satellite k are the PN code phase, τ_k , and the frequency offset, Δf_k . These can be represented by the pair $\theta_k = (\tau_k, \Delta f_k)$. The PN code sequence, $c_k(t)$, is sometimes considered a synchronisation parameter, although I do not make this distinction since the PN code sequences of the GPS satellites in view of the users are generally known.

The set of all the possible parameters is commonly named the *search space*. Its size and content depend on prior information available about the positions, velocities, and time offsets of each transmitter and the receiver. More about the size of the search space is discussed in Section 3.5.

The PN code sequences are almost always searched in parallel, in N_{ch} acquisition units called *channels*. This stems from the need to acquire at least four satellites at the same time in order to obtain a position fix. In general, the number of PN code sequences need not be the same as the number of satellites, since satellites increasingly transmit more than one GNSS signal. Here, however, I will consider that every code sequence belongs to a different satellite. Bastide *et al.* (2001), among others, treat the acquisition of multiple GNSS signals from one satellite.

Subsets of the search space of the synchronisation parameters may also be processed in parallel. This can be achieved via hardware techniques, such as massively parallel correlators (see van Diggelen, 2002), and software techniques, such as FFT-based correlation seen in Section 2.3. However, it is currently not practical to carry out a search over the entire search space in one operation, so N_w subsets, Θ_i , of the search space are employed. These subsets are often called *tiles* or *windows* in the spread-spectrum literature. We name the window which contains the correct parameters an “H1 window”; other windows are labeled “H0 windows”. Here, the model allows for only one H1 window, a simplifying assumption, which I will discuss at the end of this chapter in Section 3.6.

The time taken to process a window is called the *dwell time* and hence sets the granularity in time of the search.

The synchronisation parameters are generally estimated via the generalised likelihood-ratio test, introduced in Section 2.3. It consists in calculating the likelihood ratio, or equivalently the output of a matched filter, for all candidate parameters within a window, and retaining the parameters that produced the largest output. If the likelihood ratio crosses a pre-determined threshold β , a detector *hit* is declared.

The resulting search procedure is sometimes called a *hybrid search*. First, the signal parameters are searched within a window, one dwell time at a time. If a hit occurs, the search terminates with the synchronisation parameter estimates $\hat{\theta}_k$. Otherwise, the search continues onto the next window. If no hit has occurred after all windows have been explored, the whole process is repeated. A hit simply means that the likelihood-ratio of the parameter combination $\hat{\theta}_k$ is the largest in its subset and has crossed the detection threshold: it could be a false-alarm.

Sequential acquisition schemes, also referred to as variable dwell time, have been

studied as well as serial search strategies. These schemes try to minimize the acquisition time by performing a near continuous signal detection with a time-decreasing threshold. Some of the first results were published by Gumacos (1963), who shows how the sequential probability ratio test (SPRT) leads to the optimal acquisition time. More recently, sequential detection has been investigated for GNSS signal acquisition by Yong-Hwan Lee *et al.* (2000). The theoretical analysis of sequential acquisition is particularly difficult. O'Mahony *et al.* (2011) have recently provided some theoretical results of the sequential acquisition of GNSS signals.

In this chapter, I consider only architectures with a single, fixed, dwell time.

Theoretical analysis of acquisition time

The theoretical acquisition time of DSSS signals has been studied for many decades. Holmes *et al.* (1977) represented the acquisition process as the flow graph of a Markov chain and they were able to calculate the mean acquisition time in a single dwell-time and a double dwell-time system. Hopkins (1977) also represented the process as a Markov chain and derived similar results, for the case of a single dwell-time detector, by directly solving the Markov chain transition equations. Finally, Polydoros *et al.* (1984a,b) reviewed and unified the methods available at that date and introduced a framework often known as the *flow-graph method*. More recently, Lohan *et al.* (2004) and O'Driscoll (2007) applied flow-graph methods to the acquisition of GNSS signals. They also mention for the first time that the discrete Fourier transform can be used to calculate the full probability distributions of the acquisition time variables.

The flow graph of the search process described previously is represented in Figure 3.1. The nodes represent the different states of the acquisition process. There are $N_w - 1$ nodes of type H0 representing the H0 windows and one H1 node representing the H1 window. The shaded nodes are *absorbing* states, i.e. they are the possible final states of the search. There are three absorbing states: the D state, corresponding to a true detection; the FA|H0 state, corresponding to a false-alarm in an H0 window; and the FA|H1 state, corresponding to a false-alarm in the H1 window.

The arcs represent the possible transitions between the nodes. The transition probabilities are related to the detection probabilities, calculated at the window-level: $P_{FA|H0}$ is the false-alarm probability in an H0-window; $P_{FA|H1}$ in an H1-window; P_{MD} the probability of missed detection; and P_D the probability of detection. It is known how to calculate these probabilities and the results will be recalled in Section 3.2.

The search can start in any window i , with probability π_i . This is represented on the flow graph by the incoming arcs to the H0 and H1 nodes. It may be possible to focus

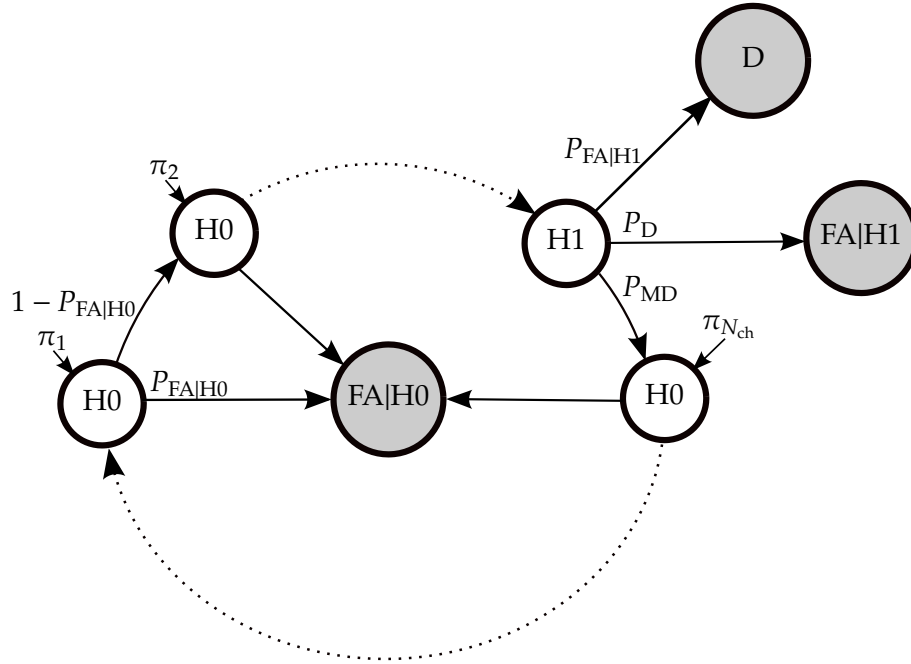


Figure 3.1: Flow graph of a single acquisition. The circles, or graph nodes, represent the different states of the acquisition process. The lines between the nodes are the transition, whose probability of occurrence is written above the line. The shaded circles represent the possible final states of the acquisition. The search can start in any of the H0 and H1 with probability π_i .

the search in the most likely windows, depending on the information available about the location of the synchronisation parameters. For example, the expanding window and the Z-search algorithms implement this strategy. In general, the search can start in any window with a uniform probability, so $\pi_i = \frac{1}{N_w}$, and I will make this assumption in the remainder of this work.

Probability generating functions

At the core of the flow-graph method is the notion of a probability generating function (PGF). The probability generating function of a discrete random variable fully characterizes the distribution of the random variable as a power series. A discrete random variable, X , taking values in $\{0, 1, \dots, M\}$ with probability mass function $P(X = m)$, has

a probability generating function defined by

$$U_X(z) = \sum_{k=0}^{\infty} z^k P(X = k),$$

with $z \in \mathbb{C}$. The definition domain C is a region of the complex plane \mathbb{C} where the series converges.

An interesting property is the relationship between the PGF of two discrete random variables and the PGF of their sum. If X and Y are two discrete random variables of probability generating functions $U_X(z)$ and $U_Y(z)$ with the same convergence region, the probability generating function of their sum is

$$U_{X+Y}(z) = U_X(z) U_Y(z). \quad (3.1)$$

This additivity property has enabled the probability generating function to become a common tool in the analysis of branching processes, arrival times, etc.

Although the probability generating function fully describes the distribution of a random variable, it is not the most convenient or intuitive way to study such a distribution. The probability mass function (PMF) or the central moments are more convenient forms of representation. The moments of the distributions, and hence the means and standard deviations, can be easily calculated from the PGF. In particular, it can be shown (see, for example, Riley *et al.*, 2006) that the expectation of X can be calculated from the derivative of the PGF evaluated at $z = 1$, if it exists, using the relation

$$\langle X \rangle = \left. \frac{dU_X(z)}{dz} \right|_{z=1}, \quad (3.2)$$

where $\langle \cdot \rangle$ is the expectation operator. If $z = 1$ is a pole of $\frac{dU_X(z)}{dz}$, the limit can be used. Similarly, higher-order derivatives of the PGF are related to the higher moments of the distribution.

Flow-graph model of single acquisition

The goal of the analysis is to calculate the distribution of the time to reach each of the possible final states of the acquisition. Holmes *et al.* (1977) and Polydoros *et al.* (1984a) showed how the probability generating functions of these times can be easily calculated from the flow graph of the acquisition process. We represent the time to reach the final states, for the n^{th} channel, by the random variables:

- $T_D^{(n)}$, the number of dwell times to reach the D state;
- $T_{FA}^{(n)}$, the number of dwell times to reach either false-alarm states - FA|H0 or FA|H1;

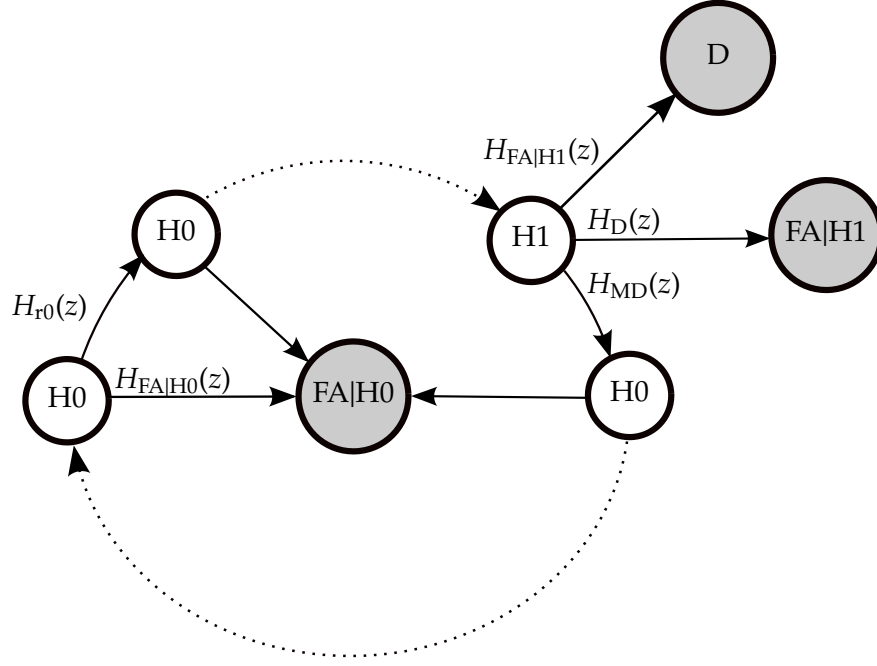


Figure 3.2: Flow graph of the acquisition process with probability generating functions. The notations are the same as Figure 3.1, where the transition probabilities have been replaced by their probability generating functions. Not pictured on the diagram, the possible entry point is any of the H0 or H1 windows with uniform probability $\frac{1}{N_{ch}}$.

- $T_{hit}^{(n)}$, the number of dwell times to reach any of the absorbing states, often called the *time-to-first-hit* (TTFH).

The flow graph of the hybrid search, expressed using the generating functions, is shown in Figure 3.2, where

$$\begin{aligned}
 H_D(z) &= P_D z, \\
 H_{r0}(z) &= (1 - P_{FA|H0}) z, \\
 H_{MD}(z) &= (1 - P_D - P_{FA|H1}) z, \\
 H_1(z) &= H_{MD}(z) H_{r0}(z)^{N_w-1}, \\
 H_{FA|H0}(z) &= P_{FA|H0} z, \text{ and} \\
 H_{FA|H1}(z) &= P_{FA|H1} z.
 \end{aligned}$$

These generating functions have been calculated by O'Driscoll (2007) for the hybrid search model and are reproduced here:

$$\begin{aligned}
U_D(z) &= \frac{1}{N_w} \frac{H_D(z)}{1 - H_{MD}(z)H_{r0}(z)^{N_w-1}} \frac{1 - H_{r0}(z)^{N_w}}{1 - H_{r0}(z)}, \\
U_{FA|H0}(z) &= \frac{1}{N_w} \left[\frac{(N_w - 1)H_{FA|H0}(z)}{1 - H_{r0}(z)} - \frac{[H_{r0}(z) - H_{MD}(z)] H_{FA|H0}(z)}{[1 - H_{r0}(z)]^2} \frac{1 - H_{r0}(z)^{N_w-1}}{1 - H_1(z)} \right], \\
U_{FA|H1}(z) &= \frac{H_{FA|H1}(z)}{N_w[1 - H_{r0}(z)]} \frac{1 - H_{r0}(z)^{N_w}}{1 - H_1(z)}, \\
U_{FA}(z) &= U_{FA|H0}(z) + U_{FA|H1}(z), \text{ and} \\
U_{hit}(z) &= U_{FA}(z) + U_D(z).
\end{aligned} \tag{3.3}$$

Inversion of probability generating functions

We could calculate the probability generating functions of $T_D^{(n)}$, $T_{FA}^{(n)}$, and $T_{hit}^{(n)}$ using the flow graph of Figure 3.1. Equations 3.1 and 3.2 could then be used to calculate the mean and the standard deviation of the acquisition time. This is the approach adopted by, for example, Polydoros *et al.* (1984a). Instead, we wish to characterize the distribution in terms of its probability mass function or its cumulative distribution function. The relationship between the probability mass function and the probability generating function is

$$P(X = m) = \frac{1}{2\pi j} \oint_C U_X(z) z^{m-1} dz, \tag{3.4}$$

where the PMF is defined over $m = 0, \dots, M$ and C is the integration contour in the complex plane, which must include all the poles of $U_X(z)$.

The integral in Equation 3.4 does not admit an analytic solution in general. Cavers (1978) showed, using the trapezoidal method, that a numerical approximation of the integral in Equation 3.4 is proportional to the inverse discrete Fourier transform (DFT), when the integration contour is a circle. In the special case where the integration is performed on the unit circle of the complex plane, the trapezoidal integration is the classical inverse DFT. A similar relationship, called the Poisson-Lattice algorithm, is given by Abate *et al.* (1992), without explicitly relating it to the DFT. Polydoros *et al.* (1984a) have also noted the relationship between the DFT and the probability generating function in their analysis of acquisition time. Holmes *et al.* (2006) used a similar method, proposed by Nuttall (1970).

I now illustrate how the method is applied. We first evaluate $U_X(z)$ at L discrete points of the unit circle $z_l = e^{2\pi j l/L}$, to form the vector $\mathbf{u} = (u_0, \dots, u_{L-1})$, where

$u_l = U_X(z_l)$. L affects the accuracy of the numerical integral and we choose $L \gg M$. The probability mass function is then approximated by

$$P(X = m) \approx \frac{1}{L} \sum_{l=0}^{L-1} u_l e^{2\pi i l m / L}, \quad (3.5)$$

for $k \in \{0, \dots, K\}$. Equation 3.5 is simply the expression for the m -th coefficient of the inverse DFT of the vector \mathbf{u} . This relationship is also known as the Poisson sum.

Equation 3.5 is used to calculate the truncated probability mass function efficiently. First, the vector \mathbf{u} is calculated. An L -point inverse DFT is then performed over the entire vector and the result gives an approximation of the PMF truncated to its first L coefficients. Since most of the probability mass of the acquisition time distribution is concentrated over short acquisition times and then becomes negligible, the truncated distribution is a good approximation of the full one.

A naive calculation of the entire PMF from Equation 3.5 would require ML evaluations of the PGF. By comparison, the DFT requires only L evaluations of the PGF, which are stored in the vector \mathbf{u} . Furthermore, the inverse DFT can be performed efficiently by implementing the inverse Fast Fourier Transform (FFT) algorithm, which is widely available in scientific software packages.

Another useful property is the relationship between the PGF of the complementary cumulative distribution function and of the probability mass function. The complementary cumulative distribution function of a random variable X is the function $P(X > x)$, which is sometimes called the tail function. We note $G_X(z)$ the generating function of the complementary cumulative distribution. $G_X(z)$ can be calculated directly from the generating function of the probability mass function, $U_X(z)$, using the relationship

$$G_X(z) = \frac{z - U_X(z)}{z - 1}. \quad (3.6)$$

This relationship is also mentioned by Cavers (1978), among others. Equation 3.6 can be calculated for the pole $z = 1$ using the l'Hopital rule, which results in $G_X(z = 1) = U'_X(1)$. Equation 3.2 shows that $U'_X(1)$ is the expectation of X , which represents the mean acquisition time in signal acquisition problems. This time has been calculated by several authors, such as Holmes *et al.* (1977), and their results can be easily re-used to provide an analytical expression of $U'_X(1)$. Equation 3.6 will often be used in the remainder of this chapter to calculate the cumulative distribution $P(X \leq k)$.

Summary of numerical calculation of inversion functions

The conversion of generating functions into distribution functions and the reciprocal transformation are the essential operations needed to build a theoretical model of an

assisted receiver. We now summarise the results from the previous paragraph and highlight the practical aspects of the numerical calculations.

The first step in finding the distribution function $P(X \leq m)$ from the generating function $U_X(z)$ is to calculate the generating function of its complementary cumulative distribution $G_X(z)$, as shown by Equation 3.6. Then we form the vector $\mathbf{g} = (g_0, \dots, g_{L-1})$ from the probability generating function $G_X(z)$ evaluated at L uniformly spaced point of the unit circle: $g_l = G_X(e^{2\pi j l/L})$. Finally, we apply the inverse FFT and transform the result to a distribution function using

$$P(X \leq m) = 1 - \text{IFFT}(\mathbf{g})(m).$$

Conversely, one can calculate L points of the generating function over the unit circle, $g_l = G_X(e^{2\pi j l/L})$ of the random variable X described by its cumulative distribution vector \mathbf{c} , with $c_k = 1 - P(X \leq k)$ using the relation

$$g_l = \text{FFT}(\mathbf{c})(l).$$

Direct derivation of acquisition distribution

DiCarlo *et al.* (1980) and Meyr *et al.* (1983) have derived an expression for the distribution function of the acquisition time of the signal from one satellite. The derivation is based on a model of the acquisition process expressed as a geometric series, whose geometric coefficient is the probability of detection P_D . This approach can also be used to calculate the distribution of the decoding time of the navigation messages, as shown by Holmes *et al.* (2006), who calculated the decoding time of the GPS P(Y) navigation message, and Anghileri *et al.* (2010) who investigated the acquisition time and frame decoding time of the Galileo signals. However, this approach is not as flexible as the inversion of the flow-graph generating function, despite being simpler. Besides, as it will be seen in a later section, the probability generating function is needed to model an assisted receiver.

3.2 Mean features of assisted-receivers models

In this section, I present the model assumptions, and in particular the specificities of assisted receivers. The goal is to identify the variables required to build a flow-graph model of an assisted receiver.

Signal search strategy

Manufacturers share little information about the architectures of their receivers. The signal search strategy is usually unknown and may be a combination of classical acquisition techniques with ad-hoc solutions. Here, we assume that the signal acquisition unit of the receiver performs a generalized likelihood ratio test, seen in Section 3.1.

The unknown frequency offset of the received signal is a combination of the Doppler offset, caused by the relative motion of the satellite and the receivers, and by the frequency bias of the local oscillator. The expected Doppler offset of the satellite is known with a good accuracy, if assistance data is available – at least for a static receiver. Hence, after detection of a first satellite, it is possible to estimate the frequency bias of the local oscillator and remove its contribution to the frequency offset search space. The size of the initial search space is therefore reduced for the acquisition of the subsequent satellites.

The acquisition process in an assisted receiver is thus a two-stage process, with two different search spaces. We will use the term *full space* to refer to the original search space, and *reduced space* to refer to the search space where the contribution of the local oscillator bias has been removed. It appears that such a two-stage architecture, where the search space sizes varies between the stages, has not been investigated previously.

We also make the assumption that the receiver has more channels available to it than the number of satellites in view, an assumption which generally holds for GPS L1 C/A receivers designed after 1990. We also assume that the detection is “single-dwell”, meaning that only one threshold crossing is required. The flow-graph method can easily include double-dwell detectors if required.

Receivers without tracking loops

The absence of tracking loops in assisted-GNSS receivers has two consequences. First, the time of transmission of the signals, which is usually decoded from the navigation message, is unknown. We have seen, in Section 2.5, that this problem is solved by adding one more unknown variable to the position equation than in conventional receivers. I therefore assumed a minimum of $K_{\text{FIX}} = 5$ satellites were needed to calculate a three-dimensional position. In Chapter 5, the minimum number of satellites required for positioning will be reduced by considering fine-time aiding and 2D positioning.

A second difficulty concerns the treatment of false alarms in assisted receivers. Conventional receivers decode the navigation message and it is then possible to check the parity field of the navigation message to detect a false alarm, with almost certainty

(see Parkinson *et al.*, 1996). On the other hand, assisted receivers generally do not decode the navigation message. Assisted receivers are designed for difficult environments, where the signal strength may be too weak to decode the data bits reliably. Furthermore, tracking loops (DLL and PLL) increase the complexity and power consumption of the receiver. Mass-market receivers sometimes do not include tracking loops at all and are therefore not able to decode the navigation message.

Assisted receivers must also detect false alarms reliably. To date, it seems that no analysis of the false-alarm rate of assisted receiver has been done and that most implementations rely on ad-hoc or heuristic methods. I was not able to find information about the treatment of false alarm in commercial receivers. Nevertheless, I assume that the detection of a false alarm is possible. One can imagine a method based on the residuals of the iterative least-squares algorithm used to calculate the position to justify that detecting a false alarm in assisted receivers is indeed possible. This least-squares positioning algorithm assumes the noise of each pseudo-range measurement is Gaussian, hence the residuals must follow a central- χ^2 distribution, with as many degrees of freedom as there are pseudo-range measurements. It may become possible to perform a statistical test on the residuals and detect a possible false-alarm if the position equation is over-determined.

I modeled a false alarm by introducing a fixed penalty time, T_{penalty} , given in numbers of dwell times, in the flow graph.

Signal model

We simplify the analysis by assuming the signal strength is constant over an entire acquisition period. A more accurate model would be a slow-fading channel, where the signal power is time-correlated. However, I was not able to include such a model in closed form in the analysis framework. Abdi *et al.* (2000), have derived analytic forms of some second-order statistics for different types of propagation channels. Fast-fading channels, in which the signal strength fluctuations are much shorter than the acquisition time, can be modelled by calculating the detection statistics (such as probability of detection and false alarms) using a parametric model of the channel. See, for example, Simon *et al.* (1998).

Detection parameters

The cell-level detector is based on a matched filter, consisting of K_{nc} non-coherent integrations of length T_{coh} , followed by a likelihood-ratio test with threshold β . The

received signal strength is C/N_0 (in normalized gain units – not dB-Hz). The dwell time is thus

$$T_{\text{dwell}} = K_{\text{nc}} T_{\text{coh}}. \quad (3.7)$$

In the Neyman-Pearson framework, the detection threshold is chosen to minimize the false alarm rate and maximize the probability of detection, at a given signal-to-noise ratio. The statistics of the non-coherent detector for hybrid architecture are given by Corazza (1996) and Borio *et al.* (2008b). The main results are recalled here.

Cell level

The equations presented in Section 2.3 are used in order to calculate the following detector statistics at the cell level: $p_{\text{FA}}(\beta)$ the probability of false alarm and $p_{\text{D}}(\beta, C/N_0)$ the probability of detection.

Window level

The window-level detection probabilities, which are those of the generalized likelihood ratio test, have been calculated by Borio *et al.* (2008b) and are recalled here:

$$P_{\text{FA}|\text{H0}} = 1 - (1 - p_{\text{FA}}(\beta))^{N_{\text{c}}} \quad (3.8)$$

$$P_{\text{MD}} = p_{\text{D}}(\beta, C/N_0) p_{\text{FA}}(\beta)^{N_{\text{c}}-1} \quad (3.9)$$

$$P_{\text{D}} = \int_{\beta}^{+\infty} (1 - p_{\text{FA}}(x))^{N_{\text{c}}-1} f_{\chi^2}(x; \lambda, K_{\text{nc}}) dx \quad (3.10)$$

$$P_{\text{FA}|\text{H1}} = 1 - P_{\text{MD}} - P_{\text{D}}, \quad (3.11)$$

where N_{c} is the number of cells in the window, $f_{\chi^2}(x; \lambda, K_{\text{nc}})$ is the PDF of the non-central χ^2 distribution of non-centrality parameter $\lambda = 2K_{\text{nc}}T_{\text{coh}}C/N_0$ and K_{nc} degrees of freedom. The integral in Equation 3.11 is evaluated numerically, using Simpson's method. The integration domain and resolution are set using a heuristic rule based on the mode and standard deviation of the distribution. I experienced some numerical precision issues when calculating the PDF of the non-central χ^2 distribution with large degrees-of-freedom (typically $2K_{\text{nc}} \gg 50$), using the Scipy scientific library. The problems were solved by using a Gaussian approximation of the non-central χ^2 distribution.

Single and multiple H1 assumptions

The flow-graph model can be completed to take into account the cases where the signal can be detected for more than one combination of parameters. For example, this is

the case if the search space has a fine resolution and the signal is strong enough to cross the threshold in many cells in the proximity of the best estimate. O'Driscoll (2007) modified the flow graph to include more than one incoming transitions to the detection state, although this method would work only for a detection in more than one window, and not at the cell level.

To resolve the case of the detection of a signal in multiple cells, Pany (2010) proposes to change the number of detector cells to reflect the possibility of than more than one cell contains the correct signal. Another approach consists in calculating the average detection statistics over several cells.

In the rest of this analysis, we assume that there is only one correct estimate of the synchronisation parameters in the entire search space.

3.3 Acquisition model of an assisted receiver

Introduction

In this section, I detail the calculation of the probability distribution of the time-to-first-fix. I present mostly new results, extending the results found in the literature reviewed in the previous section. I use the same notation $T_{FA}^{(n)}$, $T_D^{(n)}$ and $T_{hit}^{(n)}$ both for the full-space analysis and for the reduced-space analysis. Hence the distributions of these random variables are calculated using the detection parameters (number of cells, windows, threshold, and signal strength) corresponding to the acquisition stage in which they appear.

Distributions in the full-space stage

The probability generating function of the time-to-first-hit of channel n , $T_{hit}^{(n)}$, is calculated from the Equations 3.3 set to the detection parameters of channel n . We then apply the inversion method presented above to calculate the cumulative distribution $P(T_{hit}^{(n)} \leq t)$.

At the first hit occurring within any of the N_{ch} channels, the receiver enters the second stage of the acquisition process, where the search space is reduced. Mathematically, the transition time $T_{hit}^{(full)}$ is:

$$T_{hit}^{(full)} = \min \{T_{hit}^{(1)}, \dots, T_{hit}^{(N_{ch})}\},$$

which is represented by its cumulative distribution function $P(T_{hit}^{(full)} \leq t)$. The relation with the cumulative distribution functions of the individual acquisition times is

$$P(T_{hit}^{(full)} \leq t) = 1 - \prod_{n=1, \dots, N_{ch}} [1 - P(T_{hit}^{(n)} \leq t)]. \quad (3.12)$$

As noted previously, Equation 3.12 is calculated directly from the PGF of the complementary cumulative distribution function, as shown in Equation 3.6.

Distributions in the reduced-space stage

We use a similar method for the second stage of the acquisition process. First we calculate the generating functions of the each individual channel n using Equation 3.3, this time with the detection parameters corresponding to the reduced-space stage. We then invert them to calculate the distribution functions of the time to first detection, $P(T_D^{(n)} \leq t)$, and of the time to the first false-alarm, $P(T_{FA}^{(n)} \leq t)$.

There are two outcomes of interest in this stage. Either the synchronisation parameters have been correctly estimated in at least K_{FIX} channels, which guarantee a fix, or at least one detected signal is a false alarm, which will prevent the position fix. We represent the random time to reach these outcomes by $T_D^{(\text{red})}$ and $T_{FA}^{(\text{red})}$ respectively. The time to at least K_{FIX} hits, irrespective of false-alarms and detections, is labelled $T_{\text{hit}}^{(\text{red})}$ and offers some simplification of the expressions.

The distributions of these random variables can be calculated using a combinatorial approach. We denote $S_k(\Omega)$, the set of k -combinations of the elements of $\Omega = \{1, \dots, N_{\text{ch}}\}$. For example, $S_2(\{1, 2, 3\}) = \{\{1, 2\}, \{2, 3\}, \{1, 3\}\}$.

The distribution function of $T_{\text{hit}}^{(\text{red})}$ is then

$$P(T_{\text{hit}}^{(\text{red})} \leq t) = \sum_{k=K_{\text{FIX}}}^{N_{\text{ch}}} \left[\sum_{\substack{\sigma \in S_k(\Omega) \\ \omega \in \Omega \setminus \sigma}} P(T_{\text{hit}}^{(\sigma_1)} \leq t) \times \dots \times P(T_{\text{hit}}^{(\sigma_{K_{\text{FIX}}})} \leq t) \right. \\ \left. \times P(T_{\text{hit}}^{(\omega_1)} > t) \times \dots \times P(T_{\text{hit}}^{(\omega_{k-K_{\text{FIX}}})} > t) \right] \quad (3.13)$$

and the distribution function of $T_D^{(\text{red})}$ is

$$P(T_D^{(\text{red})} \leq t) = \sum_{k=K_{\text{FIX}}}^{N_{\text{ch}}} \left[\sum_{\substack{\sigma \in S_k(\Omega) \\ \omega \in \Omega \setminus \sigma}} P(T_D^{(\sigma_1)} \leq t) \times \dots \times P(T_D^{(\sigma_{K_{\text{FIX}}})} \leq t) \right. \\ \left. \times P(T_{\text{hit}}^{(\omega_1)} > t) \times \dots \times P(T_{\text{hit}}^{(\omega_{k-K_{\text{FIX}}})} > t) \right]. \quad (3.14)$$

$P(T_{FA}^{(\text{red})} \leq t)$ can be calculated with a similar combinatorial argument. However, it is simpler to use the relation

$$P(T_{FA}^{(\text{red})} \leq t) = P(T_{\text{hit}}^{(\text{red})} \leq t) - P(T_D^{(\text{red})} \leq t). \quad (3.15)$$

We use the convention that the summation over an empty set equals 1. These equations are very similar to the calculation of the order statistics of a collection of random variables.

Calculation of the overall distribution

Distributions after the reduced-space stage

The acquisition over the full-space stage stops when K_{FIX} signals out of N have been detected, giving outcomes in two different *absorbing* states:

- the false alarm state FA, where at least one of the detected signals is a false alarm, and reached with a random time of T_{FA} dwell times; and
- the true detection state D, where all detected signals are correct detections, and reached after T_{D} dwell times.

The expressions of these random times are

$$T_{\text{D}} = T_{\text{hit}}^{(\text{full})} + T_{\text{D}}^{(\text{red})}$$

and

$$T_{\text{FA}} = T_{\text{hit}}^{(\text{full})} + T_{\text{FA}}^{(\text{red})}.$$

We use the additivity property of the probability generating function, seen in Equation 3.1, to calculate the generating functions of T_{D} and T_{FA} , respectively:

$$U_{\text{D}}(z) = U_{\text{hit}}^{(\text{full})}(z) U_{\text{D}}^{(\text{red})}(z) \text{ and} \quad (3.16)$$

$$U_{\text{FA}}(z) = U_{\text{hit}}^{(\text{full})}(z) U_{\text{FA}}^{(\text{red})}(z). \quad (3.17)$$

These generating functions can be easily calculated using the inversion formula of the cumulative distribution functions presented in Section 3.1. In this case, $U_{\text{hit}}^{(\text{full})}(z)$ is calculated from the distribution function of Equation 3.12, while $U_{\text{D}}^{(\text{red})}(z)$ and $U_{\text{FA}}^{(\text{red})}(z)$ are calculated from the CDF of Equations 3.14 and 3.15 respectively.

Summary of calculations

Figures 3.3 and 3.4 summarise the steps that lead to the calculation of the generating functions required by Equations 3.16 and 3.17. The blocks $\boxed{\text{PGF} \rightarrow \text{CDF}}$ and $\boxed{\text{CDF} \rightarrow \text{PGF}}$ represent the numerical inversion functions detailed in Section 3.1.

Inclusion of the false-alarm penalty time

We stated in the previous section that we model a false-alarm by a deterministic penalty time of T_{penalty} dwell times. Its generating function is $H_{\text{penalty}}(z) = z^{T_{\text{penalty}}}$. The signal

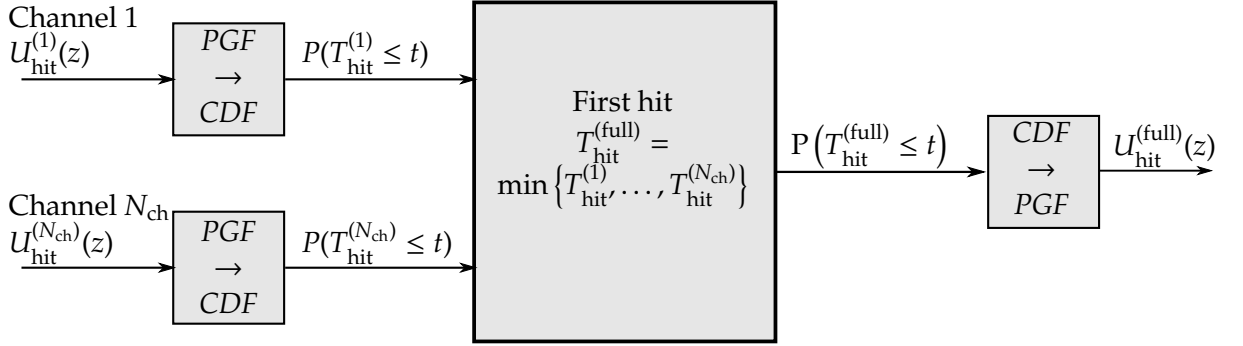


Figure 3.3: Diagram of the calculation of the theoretical time-to-first-hit at the full-space stage.

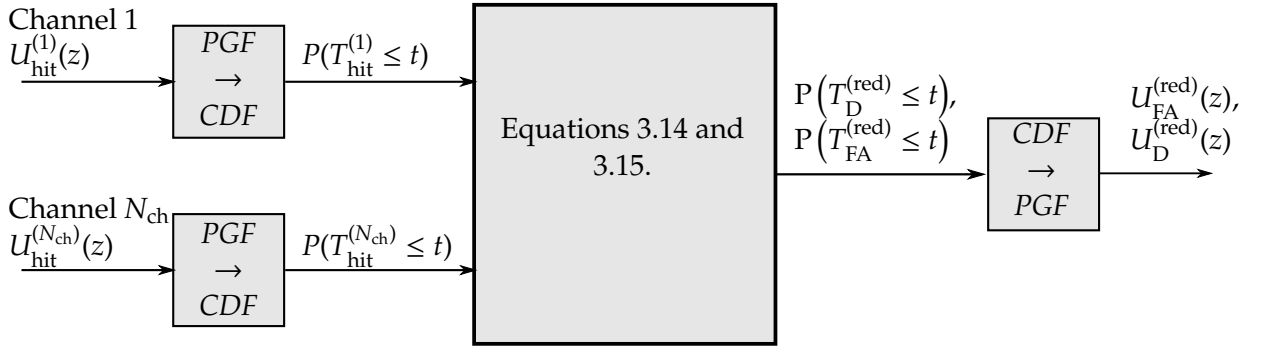


Figure 3.4: Diagram of the calculation of the theoretical time to K_{FIX} detection and time to one false alarm, at the reduced-space stage.

detected in the full-space stage is used to calculate the reduced spaces. We choose to start again the acquisitions over all K channels upon entering the reduced-space stage and the signal initially detected at the full-space stage is not tracked. This simplifies the modelling of false alarms, as false alarms can only be detected after all the satellites have been acquired.

The flow graph shown in Figure 3.5 represents an assisted receiver that can detect and recover from the false alarm state, with a fixed penalty time of $T_{Penalty}$ dwell times. The only absorbing state of this graph is now FIX, which represents the correct detection of at least K_{FIX} signals. It is reached at the random time T_{FIX} of generating function $U_{FIX}(z)$. Using the loop-reduction technique shown by Polydoros *et al.* (1984a), the

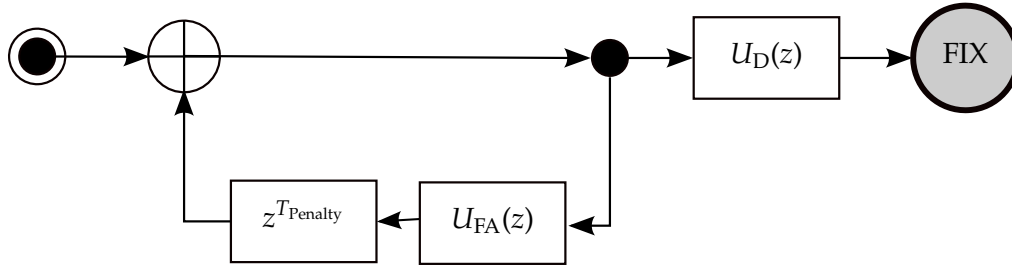


Figure 3.5: Flow graph of the assisted acquisition process with false-alarm detection and recovery.

probability generating function of the TTFF is

$$U_{\text{FIX}}(z) = \frac{U_D(z)}{1 - U_{\text{FA}}(z) z^{T_{\text{Penalty}}}}. \quad (3.18)$$

Finally, the PGF inversion method from Section 3.1 is applied to calculate the probability distribution of the time-to-first-fix, $P(T_{\text{FIX}} \leq t)$.

Model validation

We validated the theoretical model using Monte-Carlo simulations. The false-alarm rate at the cell level was chosen to be 10^{-6} , a value probably too large for a real receiver but that generated enough false-alarm events to verify the theoretical model while maintaining a reasonable simulation time.

The simulation results are presented in Figure 3.6 and show a good agreement with the theoretical model.

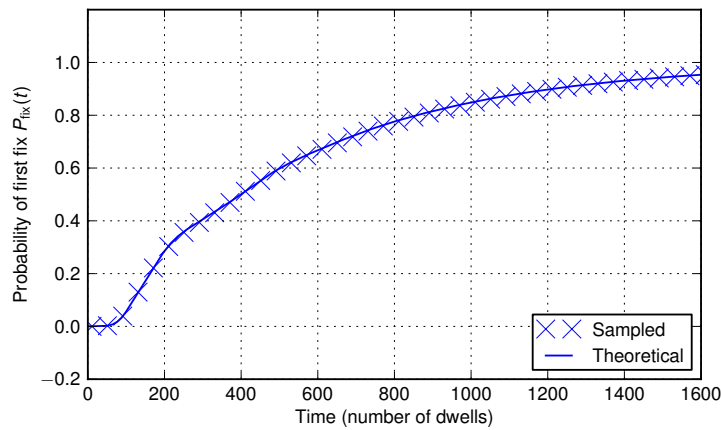


Figure 3.6: Monte-Carlo simulation of the TTFF. Plain line: theoretical TTFF. Crosses: sampled TTFF from Monte-Carlo simulations with 10^5 runs.

3.4 Illustration for typical signals

In this section, we apply the model derived previously to a simple, simulated, acquisition scenario. This provides some insight into the characteristics of the probability distributions.

Examples of TTFF distributions

I analysed the theoretical TTFF performance by considering four simple power combinations. The baseline configuration was an assisted-GPS receiver in a weak-signal environment, where eight satellites were received with a signal strength of 22 dB-Hz. The remaining configurations considered the cases of 1, 2 or 3 stronger line-of-sight signals received with a strength of 32 dB-Hz. The receiver comprised eight parallel channels, each channel having twelve windows at the full-space stage and one window at the reduced-space stage. The detector had a coherent integration period of 1 ms, which was then squared and repeated to form 300 non-coherent integrations. The dwell time was thus 300 ms. The detection threshold was set for a target probability of false-alarm of 10^{-6} . A minimum of five satellites was needed to calculate a position. A false alarm restarted the acquisition process and generated a penalty time of 600 ms.

The TTFF distributions for these four configurations are presented in Figure 3.7. The intermediate distributions are represented in Figure 3.8.

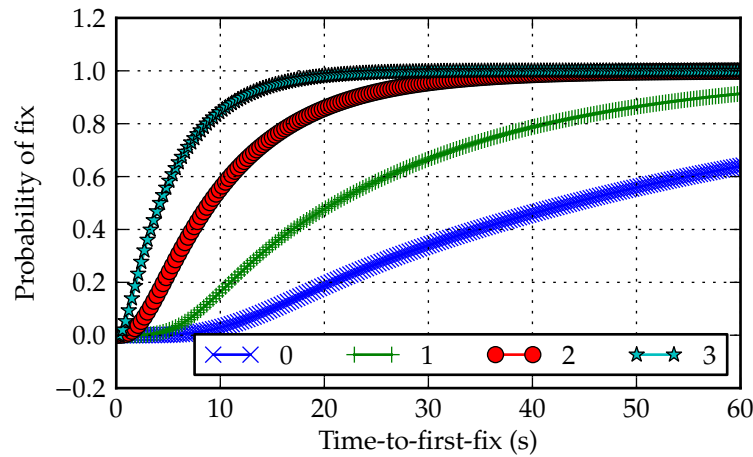
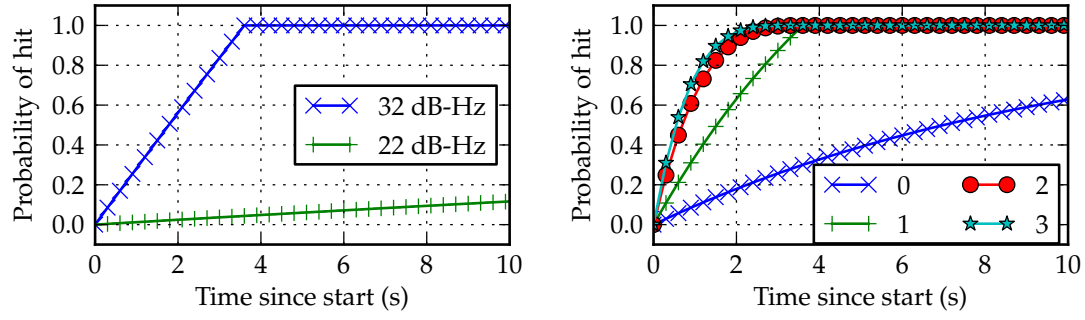


Figure 3.7: Distribution of time-to-first-fix. The value in the legend is the number of signals with a C/N_0 of 32 dB-Hz, out of 4 signals. The remaining signals have a C/N_0 of 22 dB-Hz, for a total of 8 satellites.



(a) Probability distribution of a hit on a single channel at the full-space stage. (b) Time-to-first-hit distribution at the full-space stage for each configuration.

Figure 3.8: Intermediate distributions at the full-space stage.

Analysis

The profile of the distribution function shown in Figure 3.7 can be understood by looking at the shape of the distribution at the full-space stage. In particular, Figure 3.8(a) shows that the distribution function of a single satellite is composed of linear segments. The slope of the distribution is proportional to the probability of detection, steeper slopes corresponding to stronger signals. It can be shown that the acquisition time of a single signal with a hybrid search strategy is in fact piece-wise linear, a result that was established by Holmes *et al.* (2006), using a different method. The time-to-first-hit distribution, calculated from Equation 3.12, is thus the product of piece-wise linear functions, which results in a piece-wise polynomial. This polynomial aspect is shown in Figure 3.8(b). The order of the polynomial is related to the number of signals received, with a higher order polynomial corresponding to a larger number of satellites. The coefficients of the polynomials are related to the detection probability of the signals.

The performance of the first acquisition stage is dependent on the strongest signals, and not on the total number of signals. As shown in Figure 3.8(b), the performance gain between one and three satellites with relatively stronger signals (32 dB-Hz) is small.

This is an important result for assisted-GNSS in urban environments, where only few satellites are in line-of-sight. The number of signals is not critical for the performance of the first stage. In this situation, it seems that minimizing the false-alarm rate at the first stage is more important than optimizing the time-to-first-hit. Intuitively, the multiplication of navigation signals and the parallelisation capabilities of the receivers can guarantee that the time-to-first-hit at the full-space stage is already close to being optimal. However, false alarms may have a severe impact on the overall performance, so the optimisation goal at the full-stage space should be to minimize the false-alarm

rate.

3.5 Application to real signals

The theoretical distribution of the TTFF should be compared and validated with results from a real receiver. However, an experiment supporting this comparison is very difficult to set up. We would need require an in-depth knowledge of the architecture of a receiver and run several acquisitions with a GNSS constellation simulator, which would be prohibitively time-consuming. Instead, we regulate the theoretical model with real signal-strength measurements, taken in an office.

First, we introduce the experiment performed to measure the signal strength of indoor signals. We then follow the design process of an assisted receiver: we optimize the detection parameters and calculate the search space sizes, based on the assistance data available. Finally, we present the theoretical distribution of the TTFF, as calculated using the model from the previous sections.

Indoor signals characterisation

Data collection

The direct measurement of the C/N_0 of weak signals is often not possible, since the true synchronisation parameters θ_{true} can not be estimated reliably. An alternative is to use a dual-input receiver with a common master oscillator, such as the Nordnav R30 presented by Mitelman *et al.* (2006). This configuration allows one antenna to be located in an area with a strong signal, suitable for reliable estimation of the synchronisation parameters. The other antenna can be set in a more challenging environment, where a weaker signal is expected.

Since a common oscillator provides the frequency reference for the capture of both signals, their relative phase is maintained. If the two antennas are close enough such that the code phase difference at the two locations is negligible, the true synchronisation parameters of both signals are approximately the same. A long coherent integration time can then be used to estimate the C/N_0 of the weaker signal reliably.

C/N_0 estimation

A dual-input Nordnav R30 receiver was used to estimate the C/N_0 . One antenna was positioned outdoors, on top of a building with a clear view of the sky. The other antenna was located inside an office, with an obstructed view of the sky. Figure 3.5 shows the



Figure 3.9: Overview of the office used to collect the measurements.

office and the positions of the antennas. A building faced the window and there was no direct view of the sky from the indoor antenna position.

The signal from the outdoor antenna was used to estimate the synchronisation parameters, allowing a running 200 ms coherent integration of the indoor signal. The C/N_0 was then calculated using the moments method proposed by Pauluzzi *et al.* (2000) for every satellite $p = 1, \dots, P$ acquired by the outdoor antenna. The C/N_0 estimate was then filtered with a moving-average filter of length 1 second.

The attenuation caused by the radiation pattern of the antenna is not taken into account because there is generally no line-of-sight signal indoors. We made the assumption that the indoor antenna had an isotropic pattern, even though the type of antenna used, a patch antenna, exhibited attenuation at low elevation angles.

C/N₀ results

The C/N_0 measurements were gathered in six sets of about 6.5 minutes each approximately 24 hours apart. The starting time of the acquisition was changed every day so that the satellite geometry remained the same every day. The time difference between two GPS orbital periods and a solar day was about 3 minutes and 56 seconds. The starting time was set at about 02:00 hours, when the building was empty of people.

The duration of the data collection was limited by the storage space available and the processing times.

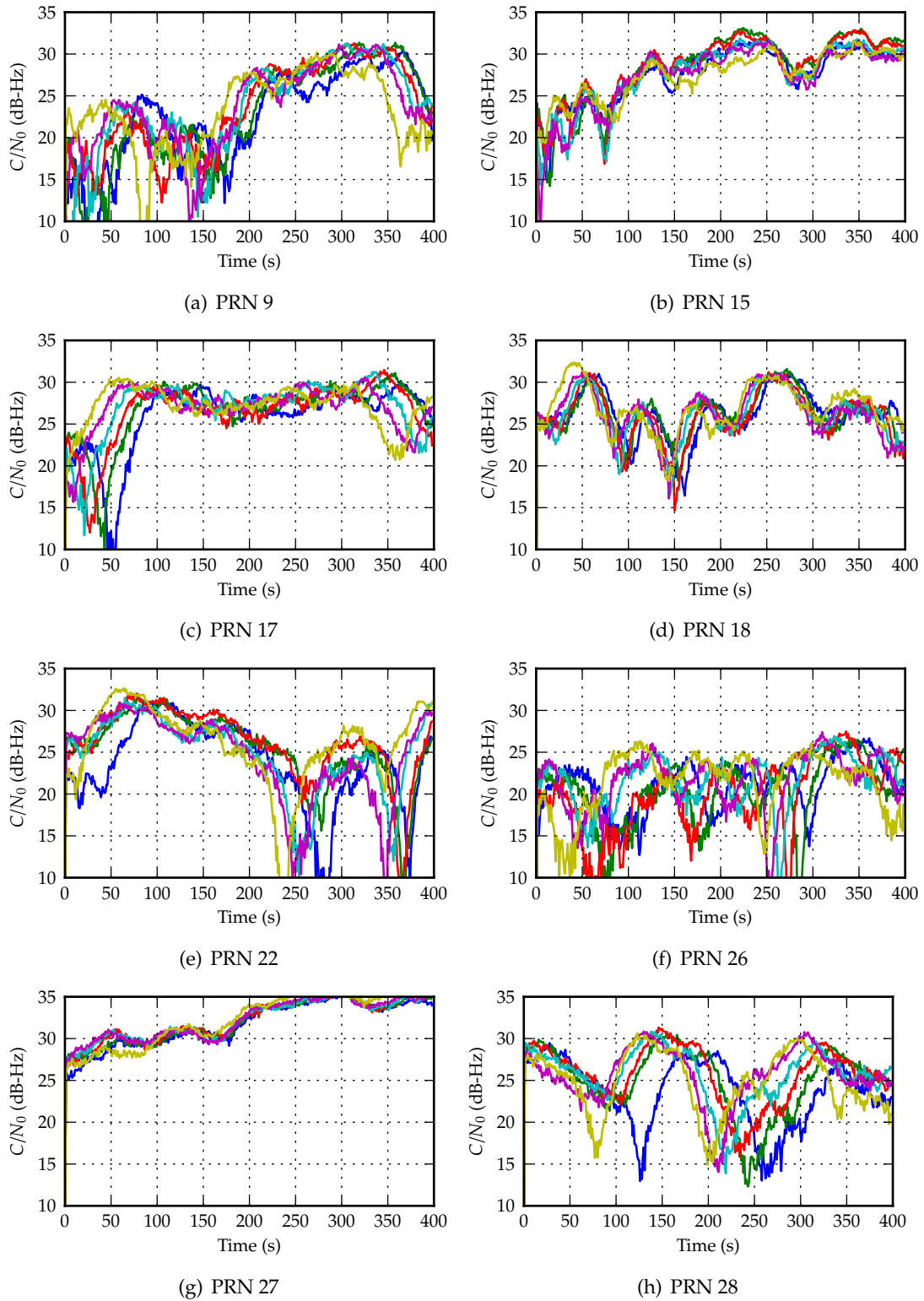


Figure 3.10: C/N_0 time series for individual satellites. Each line within one plot represents the C/N_0 recorded on a different day for the same satellite. The beginning of every time series is set to the same sidereal time.

The C/N_0 time series are shown in Figure 3.10. We observe that, for each satellite, a common fading pattern occurs every day. This pattern is probably caused by multipath fading. The indoor antenna is in a typical indoor fading environment. There is no line-of-sight with the satellites and the incoming radio-frequency signal is scattered by the building structure. The phase differences between the many scattered signals are changing with time since the satellites are moving. The phase difference introduces some fading when the scattered waves recombine at the receiver antenna.

The time series from satellites with PRN 28 and PRN 18 demonstrate that the signal strength can change by more than 10 dB in the space of one minute.

The satellites with PRN 15 and PRN 27 have the strongest signals and also have the highest elevation angles. There is no clear correlation between the elevation angle and the signal strength for the remaining satellites.

We observe a small lag between the patterns on consecutive days for each satellite. This could have been caused by a systematic error in the starting time of the acquisition, which resulted in the multipath geometry not being the same every day. It was decided not to correct this starting time offset since it was not fundamental to the rest of the analysis.

It is clear from Figure 3.11 that there is no global correlation of the signal strength of all satellites during one day.

Receiver parameters

The assistance scenarios are presented in Table 2.1 of Chapter 1. The search space limits for the three scenarios are presented in Table 3.1, using the approximations provided by van Diggelen (2002).

Table 3.1: Search space size, for each scenario.

Aiding scenario	Frequency uncertainty	Code phase uncertainty
Low level	± 4 kHz	1 ms
Medium level	± 350 Hz	1 ms
High level	± 350 Hz	20 μ s

In most situations, the probability distribution of the prior information is considered to be uniform. The uniform distribution is the simplest model representing prior information. In theory, better models could be designed for GNSS systems. For example, timing errors are not strictly uniform and can be derived more accurately from the clock model. Similarly, the user position prior distribution is not strictly

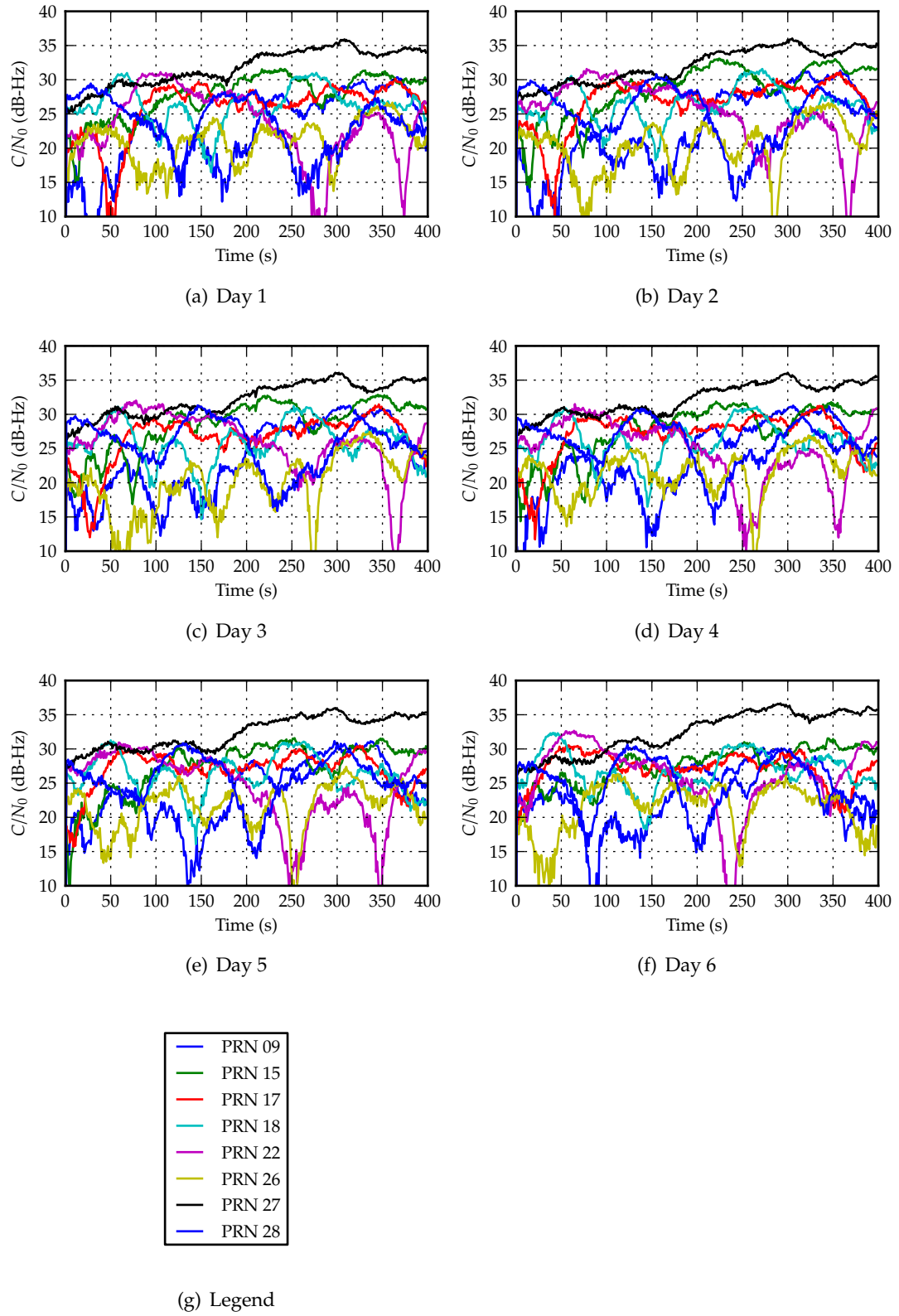


Figure 3.11: Daily C/N_0 time series

uniform. However, in practice, the uniform assumptions provides good performance and limits the complexity of the search algorithm.

Table 3.1 gives the extent of the continuous search space. Sweeping the continuous search space is feasible but not practical, since the sequences are designed such that the likelihood function of the synchronisation parameters is almost zero everywhere except in a small region close to the right parameters. We thus want to discretise the search space, with a resolution fine enough so that the correlation peak is not “missed”, but coarse enough in order to minimise the size of the discrete search space. I chose a code-phase resolution of $\Delta\tau = 1/2T_{CA}$, which limited the maximum signal attenuation to about 2.5 dB.

The frequency resolution is constrained by the coherent integration length, since coherent integration assumes that the phase difference between the incoming signal and the local oscillator is constant during the integration time. If the frequency resolution is too coarse, the mismatch between the frequency of the incoming signal and the local oscillator will introduce a systematic phase difference, which increases in time and reduces the correlation result. When the phase difference reaches 180 degrees, new samples added to the sum begin to cancel previous samples.

The relation between the frequency error, Δf , and the equivalent signal loss, L , is found in many references, for example in Stirling-Gallacher *et al.* (1996), and is recalled here:

$$L = \left| \frac{1}{T_{\text{coh}}} \frac{\sin(\pi \Delta f T_{\text{coh}})}{\pi \Delta f T_{\text{coh}}} \right|^2.$$

Ward *et al.* (2006) recommends choosing the frequency resolution

$$\Delta F_{\text{max}} = \frac{2}{3T_{\text{coh}}},$$

which limits the maximum loss to about 1.6 dB. For $T_{\text{coh}} = 1$ ms, this corresponds to a frequency resolution of $\Delta F_{\text{max}} \approx 667$ Hz.

The PRN search space is already discretised, since there are only a finite number of satellites. The resolution of this dimension of the search space generally assigns one PRN to every receiver channel. However, some search strategies work at a lower resolutions: the PRN sequences from more than one satellite are combined and both signals are searched at the same time. This approach can improve the TTFF by reducing the search space, as shown by Jan *et al.* (2009) but it can only work with strong signals because of the cross-correlation properties of the PRN sequences.

Table 3.2: Search space size, for each scenario.

Aiding	Channels	Windows	Cells
Low level	8	12	2046
Medium level	8	1	2046
High level	8	1	40

Parallelisation capabilities

We assume that the code-phase space, for all satellites and for a given frequency offset, can be searched in one dwell time. The search for a new code phase requires a new signal acquisition and thus a new dwell time. This is typical of a multi-channel receiver where the frequency-offset removal is performed in hardware and the code search is performed by a software algorithm using FFTs.

Total number of cells and windows

We can now use the size of the search space and the parallelisation capabilities established above to calculate the number of cells and windows. Table 3.2 shows the number of cells and windows of the flow graph.

Optimisation of the detector parameters

Mean acquisition time

Three parameters of the GLRT detector need to be set by the designer: the coherent integration time T_{coh} , the number of non-coherent integrations K_{NC} and the detection threshold β . The detection threshold β is directly related to the probability of false alarm at the cell level, p_{fa} , at constant noise power and integration time; it does not depend on the signal strength.

These three parameters have a direct influence on the overall acquisition performance by increasing the probability of detection. A longer integration time and a lower threshold directly increase the probability of detection. However, this increase in sensitivity has a negative impact on the acquisition time: a longer coherent integration time increases the dwell time and a lower threshold raises the false alarm rate and the number of re-initialisations of the search.

The optimal choice of these parameters is thus a trade-off between receiver sensitivity and acquisition time, for a given signal strength and receiver architecture. The detector parameters can be optimized using a numerical optimisation routine. One

approach would be to calculate a statistic, such as the mean or the 90-percentile, of the distribution of the TTFF calculated in Section 3.3, and optimize over the detector parameters. However, this solution is not practical since the computation time of the TTFF distribution would become too large for a numerical optimisation solution and there is no closed-form solution is available.

However, the mean acquisition time of a single signal is known and has a simple closed-form solution. For example, Holmes *et al.* (1977), and Polydoros *et al.* (1984a) give the closed-form expression of the mean acquisition time for a serial search. Using a symbolic calculation software, it is easy to derive a similar result in the case of a hybrid search:

$$\bar{T}_{\text{acq}} = \frac{1}{2P_D} \left((N-1)(2-P_D)P_{\text{FA}|H_0} + 2P_{\text{FA}|H_1} \right) T_{\text{penalty}} + \frac{(2-P_D)N}{2P_D} + \frac{1}{2}, \quad (3.19)$$

where \bar{T}_{acq} is the mean acquisition time expressed in number of dwell times.

Coherent integration time

The coherent integration time can be excluded from the optimisation procedure. In a matched-filter receiver, the maximum coherent integration is limited by the period of the navigation bits, and the minimum integration time by the period of the spreading code. As seen previously, the size of the frequency-offset search-space increases linearly with the coherent integration time. O'Driscoll *et al.* (2008) have studied whether the gain in receiver sensitivity was worth the increase in the search space size. They recommend the choice of the shortest coherent integration time possible. Similarly, Anghileri *et al.* (2010) considered only the shortest coherent integration time when analysing the design of a receiver. The rest of the analysis will therefore assume a coherent integration time of $T_{\text{coh}} = T_{\text{CA}} = 1$ ms.

Number of non-coherent integrations and threshold

The penalty time in Equation 3.19 is different from the penalty time introduced in Section 3.3, where the penalty time is encountered after all satellites have been acquired. Here, Equation 3.19 gives the mean acquisition time of one satellite only. Since, for an assisted receiver, a false alarm is detected only after all K_{FIX} satellites have been acquired, the acquisition time needs to be artificially increased to represent the wait for the acquisition of the $K_{\text{FIX}} - 1$ remaining satellites. Arbitrarily, I set the penalty time to five seconds; the exact value is random and depends on the implementation of the acquisition algorithm.

The average C/N_0 of the measurements, 25.8 dB – Hz, is used as the design point of the detector. As seen previously, a target window-level false-alarm rate of about 10^{-3} leads to a cell-level false-alarm of about 10^{-6} , for about 2000 cells.

Figure 3.12 shows a contour plot of the acquisition time of a single signal as a function of the number of non-coherent integrations and the probability of false alarm, for a penalty time of five seconds and over 2046 cells and 5 windows.

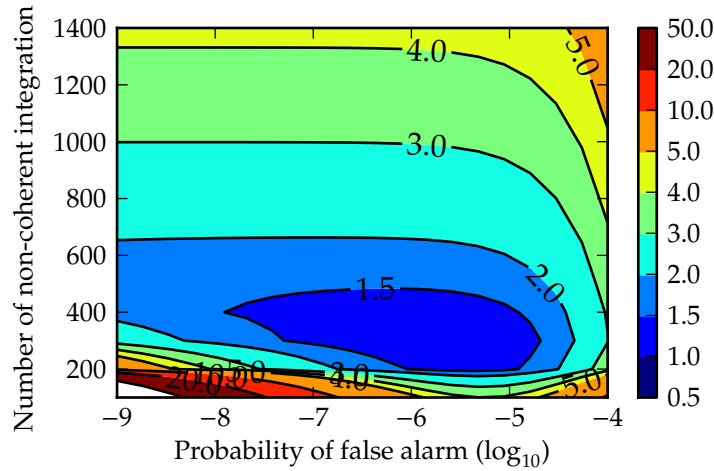
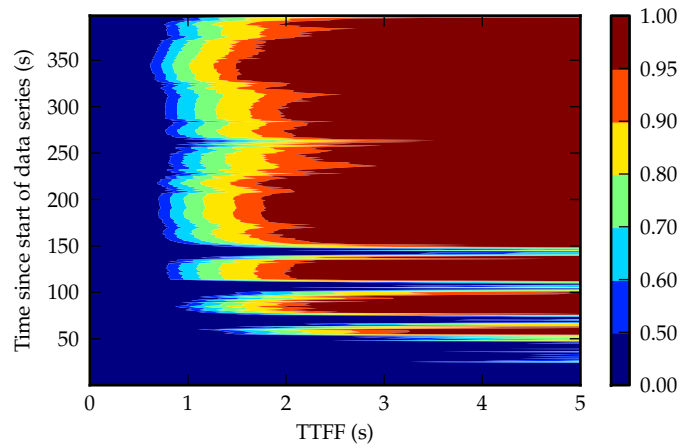


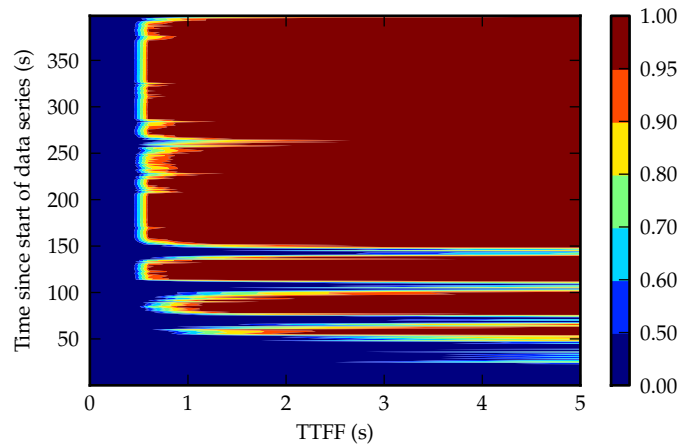
Figure 3.12: Mean time to acquisition of a single signal, in seconds. The time scale is not linear.

Three regions can be distinguished. At short integration time, the mean acquisition time is increased because of the lower probability of detection. For large number of non-coherent integrations, the probability of detection is large enough to ensure a reliable detection of the signal. The dwell time increases linearly with the number of non-coherent integrations. The mean acquisition time can become dominated by the dwell time when the number of non-coherent integration is increased. Finally, the search is slowed by an increase in the false-alarm rate, which drags the acquisition into too many false-alarm recoveries.

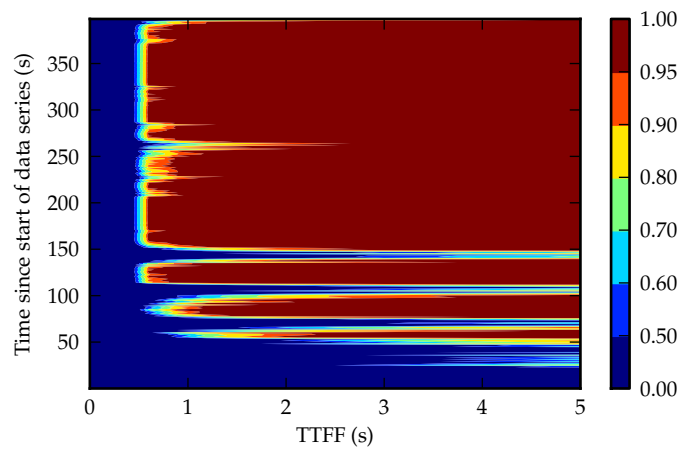
I chose a target probability of false-alarms of 10^{-6} and 400 non-coherent integrations for the rest of this analysis based on an examination of Figure 3.12. A more rigorous approach would use a numerical optimisation algorithm to calculate the optimal parameters. However I do not believe that a numerical optimisation routine would bring a significant performance improvement.



(a) Low assistance level



(b) Medium assistance level



(c) High assistance level

Figure 3.13: Contour plots of the distribution of the TTFF as a function of the starting time of the acquisition, for the signal strengths recorded on day 1. The vertical axis represents the starting time of the acquisition, where the origin is the beginning of the measurements. The horizontal axis covers the possible values of the TTFF. The probability of fix is indicated by the colour of the contour plot.

Time-to-first-fix distribution

The TTFF distribution is not constant in a fading environment, since the strengths of the signals from each satellite can vary. These variations affect the probabilities of detections and thus the acquisition times of the individual satellites. The acquisition time is increased during a fade, when the signal is weak. However, the TTFF is a function of the combinations of the signal strength of the individual satellites. Figure 3.11 shows that the signal strengths of the individual satellites are not correlated. The stationarity properties that can be observed on the individual satellites in Figure 3.10 are not present when all signals are jointly considered. The analysis of the TTFF is thus not straightforward and we choose to calculate the TTFF distribution at every time step. The evolution of the TTFF distribution as a function for the starting time of the acquisition is represented by contour plots in Figure 3.13, for the measurements taken on day 1.

Analysis

The overall TTFF performance of an assisted receiver can be significantly changed by a single satellite. This behaviour is specific to assisted receivers, where the first stage of the acquisition process relies on the acquisition of a single satellite. The second stage of the acquisition process, that requires the acquisition of $M - 1$ satellites, is more affected by the average signal strength of all satellites. This is well illustrated by looking at Figure 3.13. We observe a first period in the TTFF distribution, of about 180 seconds, where the TTFF has large variations and its median value is often more than 3 seconds, for any level of assistance. Then, from about 180 seconds to the end of the data series, the TTFF distribution becomes more regular. These two phases are understood by looking at the C/N_0 time series of all satellites, in Figure 3.11. From about 180 seconds onwards, the signal from the satellite with PRN 27 becomes clearly stronger than the other signals, thus reducing the acquisition time of the first satellite and hence the time the acquisition process spends searching the full space. This satellite has the highest elevation, more than 60 degrees and probably had the least phase difference between the reception paths, hence there was little fading.

3.6 Conclusions and future work

In this chapter, we have seen the calculation of the time-to-first-fix for the theoretical model of an assisted receiver. I applied the theoretical framework to real signal strength

measurements, taken indoors, and I calculated the theoretical probability distribution of the TTFF in this environment. The signal strength measurements highlighted the fading nature of the indoor channel, with the signal strength variations of more than 15 dB. However, the TTFF distribution was more affected by the strongest signal than the average or distribution of the other signal strengths. This is caused by the two-stage acquisition process of assisted receivers: in a fading channel, the TTFF performance depends more on the acquisition time of the first signal than of the remaining signals.

This work provides the theoretical bounds of the TTFF, at any arbitrary confidence level, for a theoretical receiver model. The theoretical bounds could be used when comparing different search strategies or during the verification and testing of navigation receivers. Another application could be to adapt the detection parameters as the search time increases. For example, one could calculate the 90%-TTFF for different types of environments, such as outdoors, urban, and indoors. Then, starting with the least challenging environment, the search strategy can adapt its parameters if no fix has been obtained after each of the theoretical bounds has been reached. Finally, the receiver could decide to stop all GNSS signal processing after the time limit for the most challenging has been reached, and thus save battery energy.

However, I believe the main interest of this chapter lies more in the mathematical tools and the approach that were used in order to calculate the TTFF distribution, than in the resulting TTFF distribution itself. The approach presented previously provides a framework that can be used to model the acquisition processes of different types of receivers. I focused on the theoretical model of an assisted receiver, but models of other types of satellite navigation receivers and, more generally, CDMA systems, could be developed.

Future work

The model assumes a slow-fading channel, where the acquisition time is shorter than the duration of the fades. The constant detector probabilities implicitly assume that the signal strength is constant between the entry point of the flow graph and the end state FIX. From the channel measurements shown in Figure 3.11, this assumption is generally valid for a static receiver. However, it is known that the crossing rate of the fades increases for a moving receiver. The theoretical model based on constant probability of detection may then overestimate the TTFF.

This limitation is difficult to resolve. If the channel model is known analytically, it may be possible to calculate the detection statistics. For example, Simon *et al.* (1998) have developed an extensive framework for the calculation of detection probability for

many fading channel models. However, this approach still assumes that the detection probabilities are time independent. Including the time correlation of the fading channel within the flow-graph method is very challenging, since a general assumption is that the probability of detection remains constant over all search windows. Corazza *et al.* (2004) analysed such a method for the acquisition time of CDMA systems and noted that the flow-graph method cannot be used in the general case of time correlation of the detection statistics. They propose a direct calculation of the acquisition, which relies heavily on combinatorial arguments.

More work should be put in the modeling of the detection of false alarms in assisted receivers. The literature of flow-graph methods almost exclusively considers a fixed false-alarm penalty time. This may not be representative of the behaviour of an assisted receiver, depending on the algorithm or mechanism used to detect false alarms. If the calculation are performed on a network server, as it is the case in the MS-assisted scheme described in Chapter 1, the penalty time depends on random parameters, such as the network load. Although I have not tried, it seems reasonably straightforward to include a random penalty in the flow graph, by simply replacing the penalty generating function of a deterministic random variable with its random counterpart, corresponding for example to a uniform distribution.

The calculation of Equation 3.14 and 3.13 can become computationally demanding as the number of channel increases. This problem is frequent in combinatorics and it could be alleviated by calculating approximate solutions. We could, for example, consider only the K satellites with the strongest signals, or we could group the satellites into sets with similar signal strength and give them appropriate weights to reflect their real cardinality. This method should give a good accuracy since the TTFF is determined by the few satellites with the strongest signals.

Time assistance from unsynchronised cellular networks

Accurate time information can help reduce the time-to-first-fix of a GNSS receiver, thus improving the user experience of mobile devices. One common method to obtain time information is to use a cellular communication network, which is accessible by many mobile devices. Many cellular networks, such as GSM networks, are unsynchronised and operators often need to deploy dedicated measuring equipment to disseminate the time information. However, we show in this chapter that the long-term stability of a GSM network could be exploited to provide accurate time assistance to a GNSS receiver, without the need for any external equipment on the network. We first review the stability properties of oscillators and I summarise the synchronisation properties of GSM networks. We present the results of experiments on the time stability of some GSM networks in Cambridge, United Kingdom. We then investigate the performance of a linear Kalman filter, combined with a two-state oscillator model, to predict the time deviations of the GSM base stations. Finally, we exploit the long-term stability of several GSM base stations to improve the accuracy of the local oscillator by building a clock ensemble filter. We demonstrate that the performance of the filter could be of practical interest to improve the time accuracy of mass-market devices.

4.1 Introduction

Motivation for reducing the search space

We have seen in the previous chapter that shortening the TTFF can be achieved by reducing the search space and by increasing the parallelisation level of the acquisition process. Massively-parallel hardware correlators, and FFT-based software correlators, have helped increase the parallelisation of the search, to the point that the all the synchronisation parameters of the GPS L1 C/A signal can currently be searched in parallel in a single dwell time by some receivers. A reduced search space may not necessarily bring a large improvement in the TTFF performance since the minimum acquisition time is limited by the dwell time, which sets the granularity of the TTFF. The dwell time, as seen in Equation 3.7, is independent of the size of the parallel search windows, hence reducing the size of the search windows may not reduce the dwell time. There are, however, at least three incentives to seek a reduction in the search space.

Firstly, the energy consumption of hardware correlators grows with the size of the search space, hence reducing the search space also improves the power efficiency of the receiver. This can be a major operational and commercial advantage in mobile devices.

Reducing the search space below the size of a search window, which is fixed by the parallelisation level of the receiver, also decreases the number of false alarms. Each false alarm degrades the TTFF since the search has to start again, which was modelled by the penalty time in the previous chapter.

Finally, GNSS receivers will have to deal with larger numbers of ranging signals in the near future, thus increasing the total search space. The periods of the PRN codes of the new ranging signals also tend to be longer, which increases the size of the search space along the code-phase axis. A longer PRN code increases the length of the coherent integration if the spreading rate is not increased. A longer coherent integration requires a finer resolution in the frequency-offset search, as we have seen in Section 3.5, which also expands the search space along the frequency offset axis. Galileo's E1 open service has, for example, a pseudo-noise period of 4092 chips transmitted at 1.023 Mchips/s, compared with 1023 chips transmitted at the same spreading rate for GPS L1 C/A. The search space for Galileo E1 open service is thus 16 times larger than for the GPS L1 C/A signal. It is possible that software receivers may have difficulties coping with such an increase in search-space size and the "real estate" cost of adding more hardware correlators may become prohibitive. Furthermore, in all cases, reducing the search space always minimizes the computational load and thus improves the power efficiency

of the receiver. This can be of prime interest in personal mobile devices.

Prior information, such as approximate position and time, can help reduce the size of the search space and is commonly used in assisted-GNSS receivers. This chapter focuses on aiding using time information only. Most mobile receivers already implement some form of frequency control, often called frequency steering, by locking the local oscillator on the RF carrier. Frequency steering does help time aiding, but the time reference of the local clock needs to be initialized. Frequency steering was designed to tune the mobile station to the RF frequency of the channel and not to provide time assistance. There is no guarantee of synchronisation between the frequencies of different base stations. Frequency steering also requires the mobile always to listen to a specific channel, which is resource demanding. A mobile receiver could manage the battery energy more efficiently by turning itself to an idle state for short periods of time. The frequency steering of the local clock may be disrupted during the energy-saving periods and time-keeping may be lost.

Previous work

Accurate time is necessary to support the operation of assisted-GNSS receivers and to develop cellular-based positioning systems. Many cellular networks, such as the GSM networks, are not synchronised by design and providing accurate time information to the network users can be challenging. Cellular network operators have deployed dedicated equipment, such as location measurement units (LMUs), to measure the time deviations of the signals in unsynchronised networks. These units are composed of receivers that measure the time fluctuations of the signals transmitted by the BTSs within their ranges, and calculate the time offsets in reference to a stable clock, such as a GPS-disciplined oscillator for example. The time information is then broadcast to the mobile users, a process generally called *time aiding* or *time assistance*. The installation and maintenance costs of this equipment can be prohibitive and an alternative, stand-alone, solution is desirable. Furthermore, the coverage of a LMU is limited to a few cells and operators may decide to deploy measuring units only over a limited portion of their networks in order to reduce costs. Therefore, mobile devices should not expect that time assistance is available everywhere.

Favey *et al.* (2001) measured the time stability of the signals from two GSM base stations. They observed that one base station was highly stable while the time deviations of the signals coming from the other BTS had periodic variations. Faragher (2007) further studied the time stability of base stations in three different GSM networks. His experimental results showed that the stability of some base stations was nearly as good

as that of an atomic frequency standard. He also observed some periodic variations of the time deviations in some networks.

These experimental measurements show that the time stabilities of GSM signals are variable across networks. However, the results suggest that some unsynchronised networks are stable enough to provide fine-time aiding. How to provide fine-time aiding from time signals in an unsynchronised network was investigated by Duffett-Smith *et al.* (2007) and described in the patent “Transfer of calibrated time information in a mobile terminal” (2010). They simulated a GSM network composed of clocks with noisy time biases and frequency drifts, which were representative of the stabilities observed during experiments. The results of their simulations showed that the local clock of a mobile receiver could keep track of the time with an accuracy better than 200 ns over a period of 300 min.

I extended the experimental work undertaken by Faragher (2007) by adding a GPS receiver to improve the long-term accuracy of the measurements. I focused on the estimation of the network clock parameters and I investigated how the stability of the networks could benefit a mobile GNSS receiver. All the results are based on measurements on real networks.

4.2 Overview of GSM signals

The signals used by a mobile device to communicate with a GSM network are described in the GSM specifications. These standardisation documents can be complex and I summarise here the parts relevant to the experiments. I also present information collected about the core networks of GSM service providers, which are not accessible for experimentation but may have an influence on the time stability.

Air interface specifications

The air interface describes the communication layers between a mobile station (MS), typically a mobile phone, and a base transceiver station. The physical layer of the air interface is specified in 3GPP (2004, TS 05.01). It is composed of physical channels on which symbols modulated by Gaussian minimum shift keying (GMSK) are transmitted at a rate of $1625/6 \approx 276.833$ kbit/s. The frequency band of a channel is specified by its absolute radio-frequency channel number (ARFCN), whose conversion to frequency is given in 3GPP (2005b, TS 05.10). The channels are allocated a 200 kHz-bandwidth and the effective bandwidth of the GSM signal is about 135 kHz after modulation and impulse filtering.

The GSM standard specifies several *logical channels* that are required for the operation of the network. The logical channels can be broadly divided into two categories, according to their usage: control channels and traffic channels. Control channels are used to support the connection of the user to the network, whereas the traffic channels carry the useful information, such as voice or data. Some channels are broadcast to all mobile stations whereas other channels, such as the traffic channels, are dedicated to transmissions with a specific user only.

The standard 3GPP (2004, p. 05.01) specifies that access to the physical layer is a combination of time-division multiple access (TDMA) and frequency-division multiple access (FDMA). These multiple access techniques are required to allow multiple communications over the same physical channel and to provide the structure for the logical channels. The TDMA part is a hierarchy of data units of various specific lengths. The most elementary unit is the *slot*, of duration $15/26 \text{ ms} \approx 576.9 \mu\text{s}$. Eight slots form a *frame*, of duration $60/13 \text{ ms} \approx 4.62 \text{ ms}$, and 51 frames form a control *multi-frame*, of duration $3060/13 \text{ ms} \approx 235.4 \text{ ms}$. A super-frame consists of 26 multi-frames and a *hyper-frame* is composed of 51 super-frames. The hyper-frame is the longest element in the GSM standard and has a period of about 3 h 28 min 54 s. The spectrum usage is optimised by FDMA, which can balance the communications over different frequency channels.

Under TDMA and FDMA, the logical channels are assigned specific time slots, frames, and frequencies by the GSM standard. The access to the channels and the allocation of the mobile stations to specific channels are both controlled by the BTSs and can be changed to adapt the radio link to the available resources. A mobile station is connected to only one BTS, which is called the serving base station. This does not prevent a mobile station from listening to other BTSs, but the GSM standard mandates that the access to the network is performed by only one BTS. Most control channels have fixed channel and frequency allocations, such that the mobile station “knows” how to discover new base stations, for example when the device is turned on or when the mobile station moves and becomes in range of a BTS offering better signal than the serving BTS.

Synchronisation of GSM networks

The multiple-access techniques TDMA and FDMA rely on the synchronisation of the mobile receiver and its serving BTS. However, the overall operation of a GSM network is unsynchronised and the time and frequency references are not synchronised between

BTSs. We review the synchronisation signals carried over the air interface and the possible synchronisation mechanisms of the core network.

The synchronisation channel (SCH) is used to achieve time synchronisation between the serving BTS and the mobile station. It transmits synchronisation bursts (SB) that contain the extended training sequence (ETS) and an encoded frame number (FN). The ETS is a known pattern of 64 bits, specified in 3GPP (2003a, TS 05.02) that has good correlation properties. The frame number contained in the synchronisation burst is encoded by a convolutional code whose parameters are given in 3GPP (2005a, TS 05.10). The synchronisation bursts also contain the base station identity code (BSIC), which is a 6-bit number identifying a base station. The SCH is a downlink control channel that is physically broadcast on the *beacon frequency channel* of every base station. The acquisition of a new BTS by a mobile station, for example when it enters the range of a new cell, is very similar to the acquisition of direct-sequence spread-spectrum signals covered in Chapter 2. The mobile station acquires the new BTS by correlating the signal on the beacon frequency channel with a replica of the ETS. Once the correlation result crosses a threshold, the mobile station can decode the information contained in the synchronisation burst. This gives the frame number that is required to synchronise the MS within the stream of frames of the channel. The position of the ETS correlation peak gives finer time synchronisation, which is required to align the transmission with the correct TDMA time slots.

The frequency of the RF carrier is controlled in order to support FDMA and to avoid interferences between adjacent radio channels. The frequency correction channel (FCCH) is used to lock the frequency of the MS to the frequency of the BTS. The FCCH consists of frequency correction bursts (FB), during which only the RF carrier is transmitted. (In reality, since differential pre-coding is applied before transmission, the data content of the burst is an alternating 0-1 pattern.) The frequency stability at the BTS shall be better than 0.05 ppm according to 3GPP (2003b, TS 05.10), for both the RF carrier and the timebase used to generate the synchronisation bursts.

GSM networks are not synchronised networks; they require synchronisation only between a mobile user and its serving base station, in order to implement TDMA. The internal counters, for instance the frame number, and the transmission time of the ETS, are not synchronised with any network time reference, but only with the local BTS oscillator. There is a provision in 3GPP (2003b, TS 05.10) to implement a pseudo-synchronised network to improve the call handovers between base stations; however the extent of the deployment of this feature is unknown.

The air interface is only one element in the networked architecture of GSM networks.

Many BTSs are typically connected together to a common base station controller (BSC), which is in turn connected to the core network of the operator. The core network, also called the network switching subsystem (NSS) in the GSM standard, provides the essential tasks of call management, signalling, and access to the public switched telephone network (PSTN). The stability of the core network and the stability of the local network around a BSC may affect the stability of the air interface. Some of these network elements may be synchronised, in particular if they are based on the synchronous digital hierarchy (SDH) protocols, which require precise time alignments of the transceivers. Some commercial brochures mention the compatibility of GSM equipment with the ITU standard G.823, whose long-term stability requirement is a maximum time deviation of $18\text{ }\mu\text{s}$ for a typical E1 link of an SDH network at 2.048 Mbit/s.

It is often claimed that improving the stability of the frequency reference at the BTS improves the overall GSM network performance. Bregni *et al.* (2003) performed experimental measurements of the call handover between two BTSs whose relative frequencies were varied between 0.1 ppm and 10 ppm. The number of calls dropped during the base stations handovers was not affected, although the study was too small to be conclusive. However, they showed a significant degradation of the speech quality, measured by the amount of speech clipping and the standardised “mean opinion score”.

Overview of W-CDMA and LTE networks

Although not central to the argument of this chapter, we review the expected performance of third and fourth generation cellular networks.

The synchronisation and timing requirements of third and fourth generation networks are not fundamentally different from GSM networks, although they are based on different technologies. The 3GPP is promoting two cellular network technologies: the Universal Mobile Telecommunication System, which is third generation network that is already widely deployed; and the Long-Term Evolution, a fourth generation network. The air interface of UMTS is called UMTS Terrestrial Radio Access (UTRA), and can be of two types: UTRA-time division duplex (UTRA-TDD), for which two-way communication is achieved by time-sharing a common physical channel, and UTRA-frequency division duplex (UTRA-FDD, more commonly named W-CDMA for wideband CDMA), where two distinct frequencies are used. The 3GPP specifies frequency accuracy requirements, for both standards, that are similar to the requirements for GSM networks. The 3GPP also specifies an global time stability of at least $2.5\text{ }\mu\text{s}$ for the TDD implementation. I have not been able to identify any major UTRA-TDD

networks in Europe and it seems that W-CDMA has been more widely deployed globally. LTE has a provision for broadcasting multimedia, which requires time synchronisation over designated areas; however, the implementation is optional.

However, many factors could improve the performance of time assistance in third and fourth generation networks. Wider signal bandwidths and improved equipment to cope with increasing traffic may improve the accuracy and the stability of time information. The channel bandwidth of W-CDMA is about 5 MHz and the bandwidth of LTE channels is flexible from 1.4 MHz to 20 MHz (with a transmitted bandwidth of 1.08 MHz to 18 MHz). A wider bandwidth improves the precision of time measurements, as seen in Section 2.1, although it does not mean that the local oscillator is more stable. On the network side, the trend in the industry seems to be to move away from circuit-switched networks and towards packet-routed networks. As the traffic increases, operators need to invest in their core networks and the current circuit-switched architectures seem too costly and not flexible enough. In a circuit-switched network, a path, or circuit, is established between the two end points for the duration of the communication. In packet-switched networks, the communication is performed by packets of information and each packet carries the address of the end point; the exact paths used by the packets are not specified and can freely change. Packet-switched networks have typically more flexible synchronisation requirements, although this is not guaranteed since packet transmission, such as the Internet Protocol (IP), can be carried on SDH synchronised networks. The problem of synchronisation over packet-based unsynchronised networks, such as IP over Ethernet networks, is under investigation by equipment manufacturers. Two technologies have been developed to this end: the synchronous Ethernet (SyncE) specifications, which sets synchronisation and stability requirements on the Ethernet protocol; and the precision time protocol (PTP) standard IEEE 1588v2, which allows sub-microsecond synchronisation over unsynchronised networks, such as Ethernet.

The impact of these factors on the stability and the synchronisation of modern cellular networks is still unclear. On the one hand, Hann (2012) shows in an industry-sponsored white paper that better synchronisation will be necessary. On the other hand, there is no requirement for global timing stability or network-wide synchronisation in the specifications of UMTS and LTE, except for the multimedia broadcasting option of LTE. The real synchronisation performance of these networks will have to be characterised experimentally. I did not investigate W-CDMA and LTE networks any further in this work.

4.3 Oscillator models and time estimation

Stability and instability of oscillators

Oscillators are electronic devices that produce a signal at a known, accurate, frequency. They are composed of a feedback loop built around a resonating element, whose natural oscillating period is precisely known. We will encounter two types of resonating elements in this thesis. Atomic frequency reference standard exploits the electronic transitions between known energy levels of atoms as their resonating elements. Rubidium frequency reference standards are a popular choice for measuring equipment, although their costs and size constraints make them less common in mass-market devices. Piezoelectric crystals, such as Quartz crystals, are often used as the resonating element in cheaper and more compact oscillators. Crystal oscillators are sensitive to temperature changes and different mechanisms are used to deal with changing temperatures. Two popular types of crystal oscillators with temperature corrections are the temperature-compensated crystal oscillators (TCXO) and the oven-controlled crystal oscillators (OCXO). TCXOs measure the component temperature and adjust the frequency in the feedback loop as a consequence. OCXOs measure and adjust the temperature of the component, using a heating element.

The most important quality of an oscillator is, arguably, its *stability* over time. But even the best atomic standards are not perfectly stable. Statistical methods to evaluate the stability of oscillators have been designed since the development of atomic clocks, in the 1960s. It is important to remember that the Coordinated Universal Time (UTC) cannot be observed directly, hence the performance of an oscillator is always measured in comparison with another oscillator. The measurements of instabilities are generally the phase differences, $\phi(t)$, between two oscillators under study, both of nominal frequency f_0 , measured at time t in the reference oscillator time scale. One can also calculate the time deviation $x(t) = \frac{\phi(t)}{2\pi f_0}$ from the phase difference and the normalized frequency deviation $y(t) = \frac{dx(t)}{dt}$.

The power spectral density (PSD) of the normalized frequency deviations can be used to characterise the statistics of the instabilities in the frequency domain. The different sections of the PSD plot show the noise processes involved in the instabilities. These are:

- a white Gaussian phase noise, of PSD slope f^2 ;
- a flicker phase noise, of PSD slope f ;
- a white Gaussian frequency noise, which is also a random walk phase noise, of PSD slope 1;

- a flicker frequency noise, of PSD slope $1/f$;
- and a random walk frequency noise, of PSD slope $1/f^2$.

The flicker noise process, or pink noise, is a type of noise process whose power spectral density follows a $1/f$ function. Its origin is generally less understood than Gaussian noise or random walk noise, although it has been observed in many types of oscillators. Flicker noise can cause some statistical estimators to diverge, for example when estimating the autocorrelation function. The lack of an estimator of the autocorrelation function can be a problem since it is generally more convenient to characterise the stability of an oscillator over a period of time than in the frequency domain. The *Allan variance*, or the *Allan deviation*, was introduced by Allan (1966) to provide a measure similar to the autocorrelation function, which can be used to study the noise characteristics of clocks in the time domain. It is defined as the two-sample variance of the normalized frequency,

$$\sigma_y^2(\tau) = \frac{1}{2} \left\langle \left(y(t+\tau) - y(t) \right)^2 \right\rangle,$$

and can also be expressed using the time deviations as

$$\sigma_y^2(\tau) = \frac{1}{2\tau^2} \left\langle \left[\left(x(t+2\tau) - x(t+\tau) \right) - \left(x(t+\tau) - x(t) \right) \right]^2 \right\rangle,$$

where $\langle \cdot \rangle$ is the expectation operator.

This Allan variance can be estimated from N samples of the time deviations measurements by the *sample* Allan variance, defined as

$$\hat{\sigma}_y^2(\tau) = \frac{1}{2(N-1)\tau^2} \sum_{k=1}^{N-1} \left(x(kT_s + 2\tau) - 2x(kT_s + \tau) + x(kT_s) \right)^2,$$

where T_s is the sampling period of the input signal.

Table 4.1: Characteristics of the noise processes in the power spectral density and the Allan variance plots, using log-log axes.

Type of noise	Allan variance	PSD
White phase noise	$\propto \tau^{-2}$	$\propto f^2$
Flicker phase noise	$\propto \tau^{-2}$	$\propto f^1$
White frequency noise	$\propto \tau^{-1}$	$\propto 1$
Flicker frequency noise	$\propto 1$	$\propto f^{-1}$
Random walk frequency noise	$\propto \tau$	$\propto f^{-2}$

The slopes of the noise processes are presented in Table 4.1, both for the Allan variance and the PSD. We can see in this table that the standard Allan variance cannot

differentiate between the flicker and white phase noise. The *modified* Allan variance has been proposed to take into account the flicker noise. As seen later, the model considered in this chapter simply ignores the flicker noise, thus the modified Allan variance is not investigated any further.

The stability is often quantified by the h -parameters of the oscillator, which are related to the magnitude of the power spectral densities of the different noise processes. The standard IEEE STD 1139 specifies the relationship between the total power spectral density, $S_y(f)$, and the h -parameters:

$$S_y(f) = \sum_{\alpha=-2}^2 h_{\alpha} f^{\alpha}.$$

Table 4.2 is reproduced from Brown *et al.* (1997, chapter 11) and shows the typical noise parameters of three types of oscillators. The long-term stabilities of the oscillators are determined by the white frequency noise, characterised by the h_{-2} parameter. Table 4.2 shows the magnitude of the noise power spectral density changes by about nine orders of magnitude between a Rubidium frequency standard and a TCXO. Rubidium oscillators are typically an OCXO locked onto the frequency of a Rubidium frequency standard. The short-term stability of Rubidium oscillators is thus the stability of the OCXO oscillator.

Table 4.2: Noise parameters of typical oscillators.

Oscillator	h_0	h_{-1}	h_{-2}
TCXO	2×10^{-19}	7×10^{-21}	2×10^{-20}
OCXO	8×10^{-20}	2×10^{-21}	4×10^{-23}
Rubidium	2×10^{-20}	2×10^{-24}	4×10^{-29}

The oscillator sensitivity to the environmental conditions is perhaps as important as its stability in ideal conditions. Even the temperature compensation of TCXO and the temperature control of OCXO may not be enough to guarantee the same stability performance across a wide range of operating temperatures. The sensitivity to temperature of a typical mass-market TCXO is between 0.1 ppm/°C and 0.5 ppm/°C.

Oscillator models

We now wish to build an oscillator model that includes the noise processes discussed previously. We adopt a state-space approach, which is compatible with many forms of recursive Bayesian estimation, such as the Kalman filter. Van Dierendonck *et al.* (1984)

treated this approach in detail and proposed the two-state oscillator model, which is frequently used in the GNSS literature.

The flicker noise cannot be represented in a state-space model with additive Gaussian noise. We can understand this problem by remembering that the state-space representation of a linear system is, informally, an expression of the linear relationships between the state vector and its first derivatives, with additive Gaussian noise (see Section 2.1). It can also be viewed as the matrix representation of a set of first-order linear stochastic differential equations with Gaussian noise. The Gaussian noise term is applied to the first-order derivative of the state vector and is then integrated when the system is solved for the state vector. The integration of the Gaussian noise leads to a random-walk noise, thus informally “skipping” the flicker noise model. This results is well-known and several authors have proposed different approach to treat the flicker noise in state-space models. Van Dierendonck *et al.* (1984) approximate the flicker noise contribution by increasing the variance of the other noise and Davis *et al.* (2005) model the flicker noise by a linear combinations of Markov processes.

Several models of oscillators have been proposed and we consider a simple model with a state vector of two elements. The time deviations are modelled as a linear combination of an integrated random walk and a random walk. We use a state-space representation with the state vector $\mathbf{x}(t) = [b(t), \dot{b}(t)]^T$, where $b(t)$ is the time deviation and $\dot{b}(t)$ the clock drift rate. The evolutions of the oscillator are described by the linear equation:

$$\mathbf{x}(t_{k+1}) = \begin{bmatrix} 1 & t_{k+1} - t_k \\ 0 & 1 \end{bmatrix} \mathbf{x}(t_k) + \mathbf{w}(t_{k+1} - t_k), \quad (4.1)$$

where $\mathbf{w}(t)$ is a Gaussian random noise process with covariance matrix $Q(\Delta t) = \langle \mathbf{w}(\Delta t) \mathbf{w}(\Delta t)^T \rangle$.

The process covariance matrix $Q(\Delta t)$ contains information about the noise characteristics of the oscillator. We have already seen that the h -parameters characterise the instabilities in the frequency domain. Similarly, the diffusion parameters q characterise the instabilities in the time domain. The literature about the relationship between the h -parameters and the diffusion parameters, and between the h -parameters and the process covariance matrix, is at times confusing. Van Dierendonck *et al.* (1984) derived the process covariance matrix from the Allan variance parameters and their result was later corrected by Brown *et al.* (1997). Zucca *et al.* (2005) calculated that the corrected covariance matrix, Q , is

$$Q(\Delta t) = \begin{bmatrix} q_0 \Delta t + q_{-2} \Delta t^3 / 3 & q_{-2} \Delta t^2 / 2 \\ q_{-2} \Delta t^2 / 2 & q_{-2} \Delta t \end{bmatrix}, \quad (4.2)$$

where Δt is the time interval of the process evolution and q_0 is the coefficient of the random walk of the phase noise process and q_{-2} the coefficient of the random walk of the frequency noise process.

We can identify the q -parameters from the previous expression with the frequency-domain h -parameters. Pany (2010) states that the process covariance matrix given by Van Dierendonck *et al.* (1984) in terms of h -parameter is incorrect. He recommends the expression given by Brown *et al.* (1997),

$$q_0 = h_0/2 \quad \text{and} \quad (4.3)$$

$$q_{-2} = 2\pi^2 h_{-2}. \quad (4.4)$$

Chaffee (1987) presented similar results for a three-state oscillator model, which includes a random-walk frequency drift, or frequency ageing. The noise density of the random-walk frequency noise was further corrected by Zucca *et al.* (2005), who also show that the Allan variance of an oscillator with a random-walk frequency drift is not stationary and depends on a reference time.

4.4 Time stability of the GSM air interface

In this section, we measure the times of arrival of the synchronisation signals from several GSM base stations in Cambridge, United Kingdom. Faragher (2007) made similar experiments to measure the stability of the BTS clocks and I repeated his experiments to obtain recent measurements. I extended his experimental arrangement by adding a GPS software receiver, which provided UTC time measurements.

Experimental apparatus

The experimental arrangement consisted of a GSM receiver, a GPS receiver, a synchronisation mechanism, and data storage units. It is schematically presented in Figure 4.1.

An IFR 2319e signal analyser received the GSM signals. The input of the analyser was connected to an outdoor GSM 900/1800 MHz monopole antenna via a low-noise amplifier (LNA) with an approximate gain of 23 dB. The signal analyser had a general purpose interface bus (GPIB, normalised as IEEE-488) which could be accessed from a remote computer. A laptop computer was used to send GPIB configuration commands to the signal analyser. The signal analyser stored the GSM samples in its internal memory and a computer equipped with a National Instrument NI AT-DIO-32HS digital input/output card regularly retrieved the samples using a dedicated high-speed

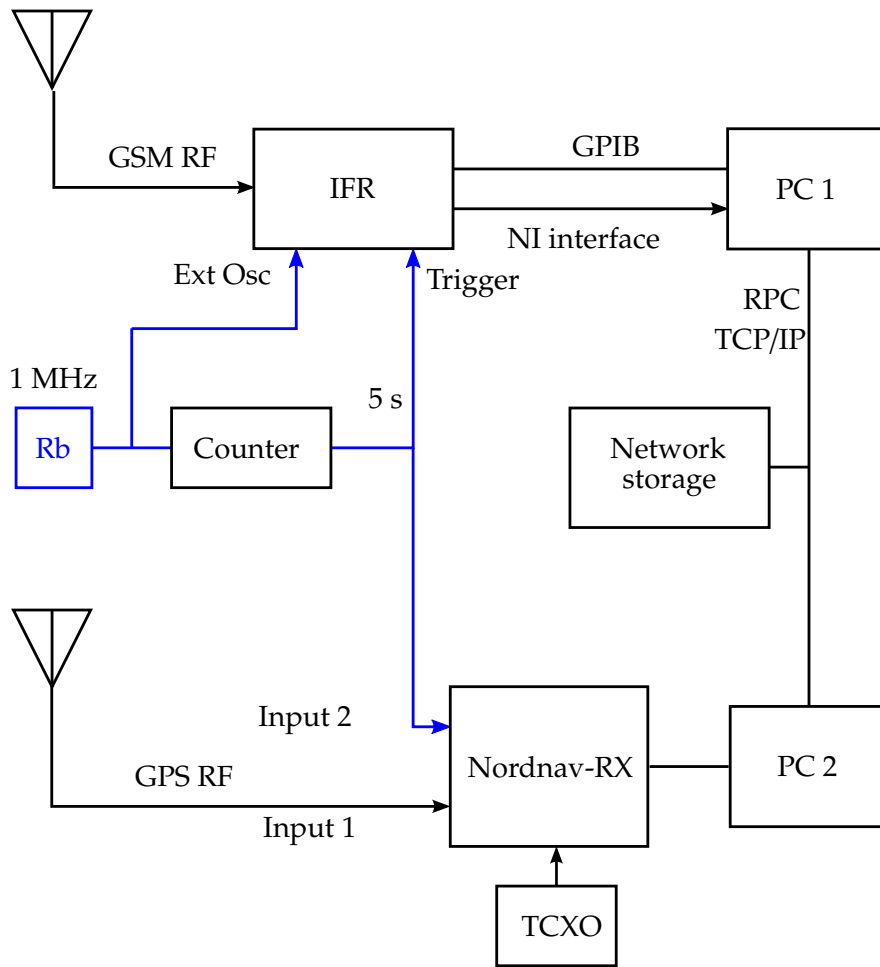


Figure 4.1: Schematic diagram of the experimental arrangement using a Rubidium frequency reference standard. The diagram does not represent the real physical location of the components.

parallel interface. The analyser's oscillator was locked to an Efratom FRK-H Rubidium frequency reference standard. I did not need the stability offered by the Rubidium frequency standard since the GPS time was also measured, but having a stable frequency between GPS measurements facilitated the signal processing.

The GPS receiver was a Nordnav R30 receiver, developed and described by Mitelman *et al.* (2006), which was controlled by a laptop computer running a dedicated program. The receiver was connected to a GPS patch antenna via a LNA with a gain of about 20 dB. The receiver did not have an external oscillator input and I left the internal TCXO oscillator as its frequency standard.

A trigger signal synchronised the recording of the GPS and GSM signals. It was generated by the digital counter of a Measurement Computing PC-CARD-D24/CTR3

card. I configured the counter to provide a square wave of 5-second period when connected to the Rubidium frequency standard. The trigger signal was connected to the trigger input of the IFR 2319e. The Nordnav R30 GPS receiver did not have an external trigger input. It had two inputs synchronised by a common clock and I bypassed the RF frontend of the second input so that it accepted the trigger signal. A program was run during post-processing to synchronise the GPS measurements acquired on the first input with the trigger signal on the second input. The GPS receiver was started before the trigger signal was sent, so that the transition of the trigger signal was always among the samples recorded on the second input of the receiver.

The receivers could not acquire data continuously because of data storage and bandwidths issues. I developed programs in C++ to control the sequencing of the measurements. The laptop computer A ran a program to control the GSM analyser via its GPIB interface. The laptop computer A also ran the software provided by Nordnav to control the GPS receiver. I developed a dynamic-link library that was plugged in the Nordnav software and that provided a software trigger to start and stop the GPS receiver. The computer B ran a program that configured the counter, kept track of the list of GSM beacon channels to measure, and called other programs using XML-RPC to sequence the recording events. XML-RPC is a network protocol to call procedures on remote machines and I used the XmlRpc++ implementation (see Morley, 2003).

A software timer on the computer B started the recording sequence at intervals of about 7 minutes. This period was chosen as a compromise between the high sampling rate desired for accurate signal analysis and the low total number of samples imposed by the storage space and processing time limitations. The recording sequence was as follows:

1. The computer B transmitted the new beacon channel frequency in the list to the laptop computer A. It then waited for new samples on its digital input/output interface.
2. The laptop computer A configured the IFR 2319e signal analyser with the new frequency and armed the trigger. It sent an acknowledgement message to the computer B.
3. The trigger signal started the acquisition and the samples were transferred to the computer B. The laptop computer A also sent a verification message to ensure the RF frequency, set by computer A, was the one corresponding to the acquisition requested by computer B. This avoided skipping beacon channels because the acquisition buffer of the signal analyser had overflowed.
4. The laptop computer B saved the samples contained in the digital input/output

buffers and repeated the sequence with the next beacon channel frequency. The laptop computer A also started the GPS receiver for a period of 30 seconds at the beginning of the sequence. The files were automatically transferred to a network storage drive at regular intervals.

The base sampling rate of the IFR 2319e signal analyser was 65.28 MHz and an IQ decimation ratio of 32 was chosen to maximise the recording length. This gave an effective IQ sampling rate of 2.040 MHz. The buffer was limited to 10^6 IQ samples, which was about 490 ms of baseband samples at the chosen sampling rate. The synchronisation burst was sent five times in a multi-frame, resulting in either ten or eleven extended training sequences available in each sampling buffer. The Nordnav GPS receiver recorded real 4-bit samples at the intermediate frequency (IF) of 4.1304 MHz and with a sampling rate of 16.3676 MHz. I established a list of the beacon frequencies of twelve different base stations, although the signal strengths of some of these BTSs were not strong enough to be fully exploited.

Calculating the times of transmission of the GSM synchronisation bursts

I used the information contained in the synchronisation bursts to calculate the times of transmission of the GSM signals, $t_i^{(GSM)}(t)$, given in the time scale of the base station i and measured at the instant t in the local time scale. The TOT was determined from the position of the ETS in a burst and from the frame number, which identified the position of the burst within a hyper-frame. The GSM standard does not define any time origin of the signals; the only time origin we can extrapolate from the information provided in the synchronisation burst is the origin of the current hyper-frame. The time origin of the TOT measurement was thus the beginning of the hyper-frame containing the burst.

The first operation required to estimate the TOT is to measure the arrival time of the ETS within a time slot. I used a method similar to the estimation of the code phase of a pseudo-noise signal presented in Section 2.1. The correlation function was calculated with the computationally efficient FFT-method, described in Section 2.3 and I up-sampled the baseband signal ten times in order to improve the resolution of time measurements. Upsampling improves the accuracy only if the signal bandwidth is perfectly limited to the Nyquist sampling frequency of 2.040 MHz. In practice, the signal bandwidth was affected by multipath and interference, so the accuracy of the time measurements on the upsampled signal may not have been as high as ten times the original accuracy. However, I upsampled the signals as it provided a better resolution that may have been useful when the results were filtered. I calculated the cross-correlation function of the upsampled signal with an upsampled replica of the

ETS, in order to detect the signal using the likelihood-ratio test presented in Section 2.2. I rejected the measurement if the squared-magnitude of the correlation peak was below a threshold and then proceeded with the next burst. Otherwise, I measured the position of the correlation peak relative to the burst, which gave the fractional part of the TOT, or the TOT modulo one time slot.

The second operation is to calculate the position of the synchronisation burst within a hyper-frame. I estimated the channel impulse response from the correlation profile of the ETS sequence with the original (not up-sampled) signal. I then filtered the signal with a channel equalizer configured for the channel impulse response. The equalization step was not strictly needed but it provided a better error-free decoding rate for weak signals. The encoded bits of the burst were recovered and the convolutional encoding was removed by passing the bits through a Viterbi decoder of rate 1/2 and with polynomials $D^4 + D^3 + 1$ and $D^4 + D^3 + D + 1$, where D is the delay operator. The frame number was reset at the beginning of every hyper-frame, which occurred about once every 3 h and 30 min. The time of transmission of the burst was given by the frame number with a granularity of one time slot. (The frame number had a granularity of a TDMA frame, but the synchronisation burst always occupied the same time slot within a frame, hence the granularity was a time slot). The fractional TOT, calculated from the position of the correlation peak, was added the TOT of the time slot to give the time of arrival, $t_i^{(GSM)}(t)$. I also decoded the BSIC contained in the synchronisation burst, which was compared with the theoretical BSIC of the BTS in order to discard the bursts that have not been decoded properly.

I developed a software GPS receiver to retrieve the GPS system time from the samples recorded by the Nordnav R30 receiver. The navigation data was decoded in order to detect the preamble and the time-of-week words. I did not decode the entire ephemeris; it was downloaded from the International GNSS Service (IGS, see Dow *et al.*, 2009) instead. The positions of the TOW words gave the pseudo-range measurements for the position equation. I further constrained the position equation by fixing the three position variables to the position of the GPS antenna, estimated from a 12 h-position average. I solved the position equation for the receiver time bias, which was the only remaining unknown. The equation was over-constrained since there were typically six to eight pseudo-range measurements and only one unknown variable.

The decoding of the synchronisation bursts was not free of errors, even though the Viterbi algorithm corrected most of them. An error in decoding one of the bits encoding the frame number could introduce large time-of-arrival errors. I developed a heuristic algorithm to detect large outliers, based on the comparison between the time

of transmission of a given burst and the median time of transmission of its neighbours. The outliers were then removed and excluded from further processing.

I observed two time jumps of about -1.2 s and 2.7 s in all the time measurements, the first one appearing about 16 s after the start of the experiment and the second occurred about 30 min later. I did not observe the same jumps on the GPS measurements, which therefore excluded a problem with the frequency reference standard. The problem did not seem to have been caused by the counter either, since the durations of the jumps were unrelated to the period of the trigger signal or any power-of-two multiple of the base timing signals. The delay appeared simultaneously on all the BTS measurements, thus making a single BTS unlikely to be the cause of the problem. The remaining possibility was a problem of signal acquisition by the IFR 2319e. It was, however, surprising that the same delay appeared at the same time on all frequencies and lasted for several acquisitions. A problem with the triggering or the acquisition buffer of the IFR 2319e should have lasted for only one acquisition. I was not able to determine the origin of these jumps. So I corrected them by introducing artificial offsets in the measurements. I repeated the experiment for the work presented later in this chapter, in Section 4.6, and I did not observe any jumps in that experiment.

I estimated the ageing of the Rubidium frequency standard from the time difference between the first and last GPS measurements, $t^{(GPS)}(t_1) - t^{(GPS)}(t_0)$, and the same time difference according to the Rubidium frequency standard, $t_1 - t_0$. I estimated a frequency ageing of 3.31×10^{-10} , which was within the specifications of the equipment. I applied this correction to all the measurements derived from the Rubidium frequency standard, for example the times of arrivals of the GSM signals.

Measured time deviations of GSM synchronisation bursts

The timing results were filtered by a Kalman smoother to remove a few remaining outliers. The Kalman smoother was not used as a statistical estimator but simply as a tool to remove the remaining outliers and produce a better visualisation of the results. I chose a two-state oscillator model with a large process noise variance, corresponding to the h -parameters $h_0 = 10^{-16}$ and $h_{-2} = 10^{-17}$. The large process noise variance ensured that the filter kept the information from the measurement intact while rejecting the largest outliers. I also considered a simple random-walk process model but the two-state oscillator model had the advantage of also estimating the frequency drifts. I tried other values of the h -parameters to make sure the smoother was neither over-fitting nor smoothing the results too much.

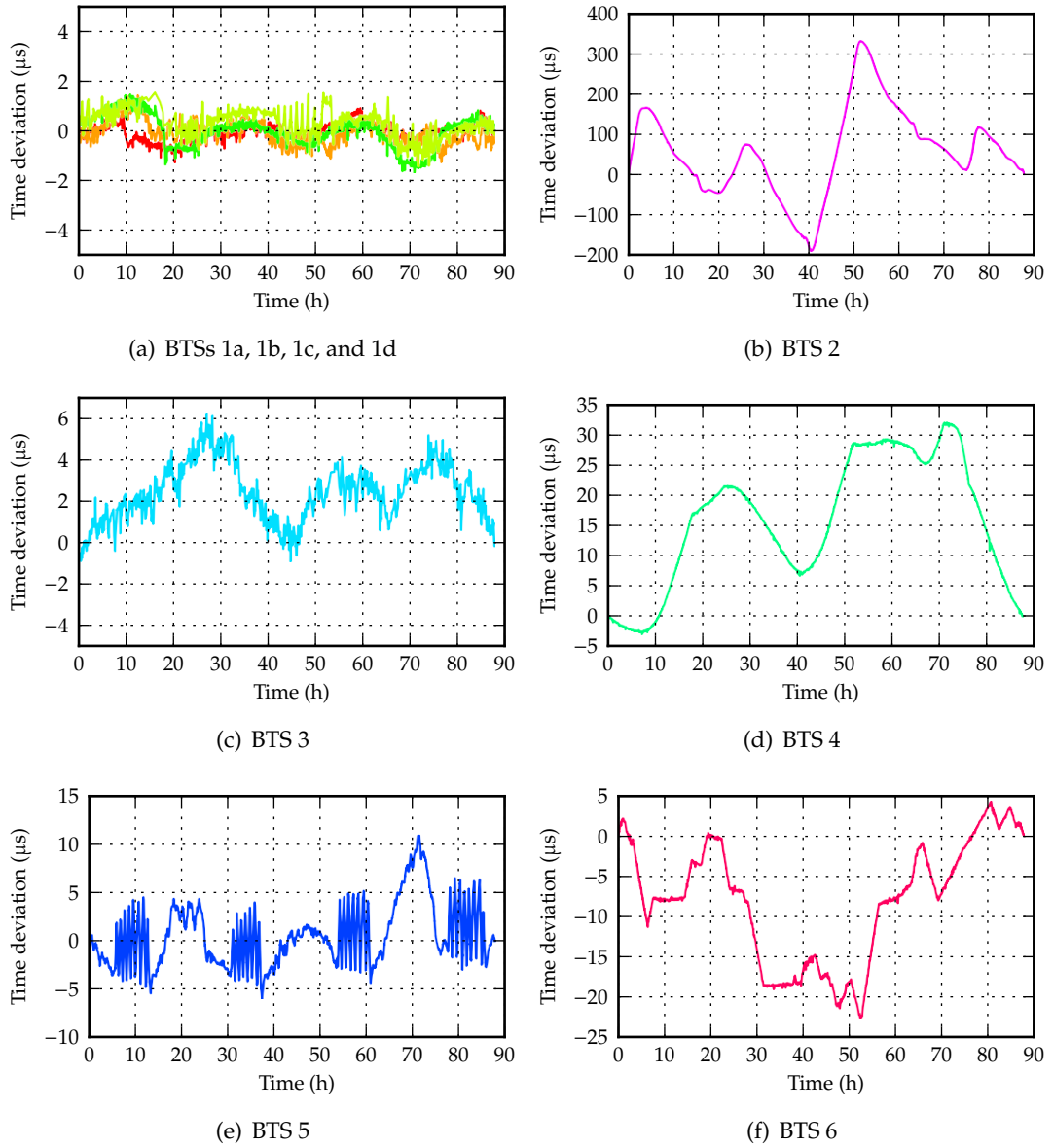


Figure 4.2: Estimated times of arrival of the synchronisation bursts from the BTSs. The results have been smoothed, centred by removing the arrival time of the first sample, and detrended with the average drift rate.

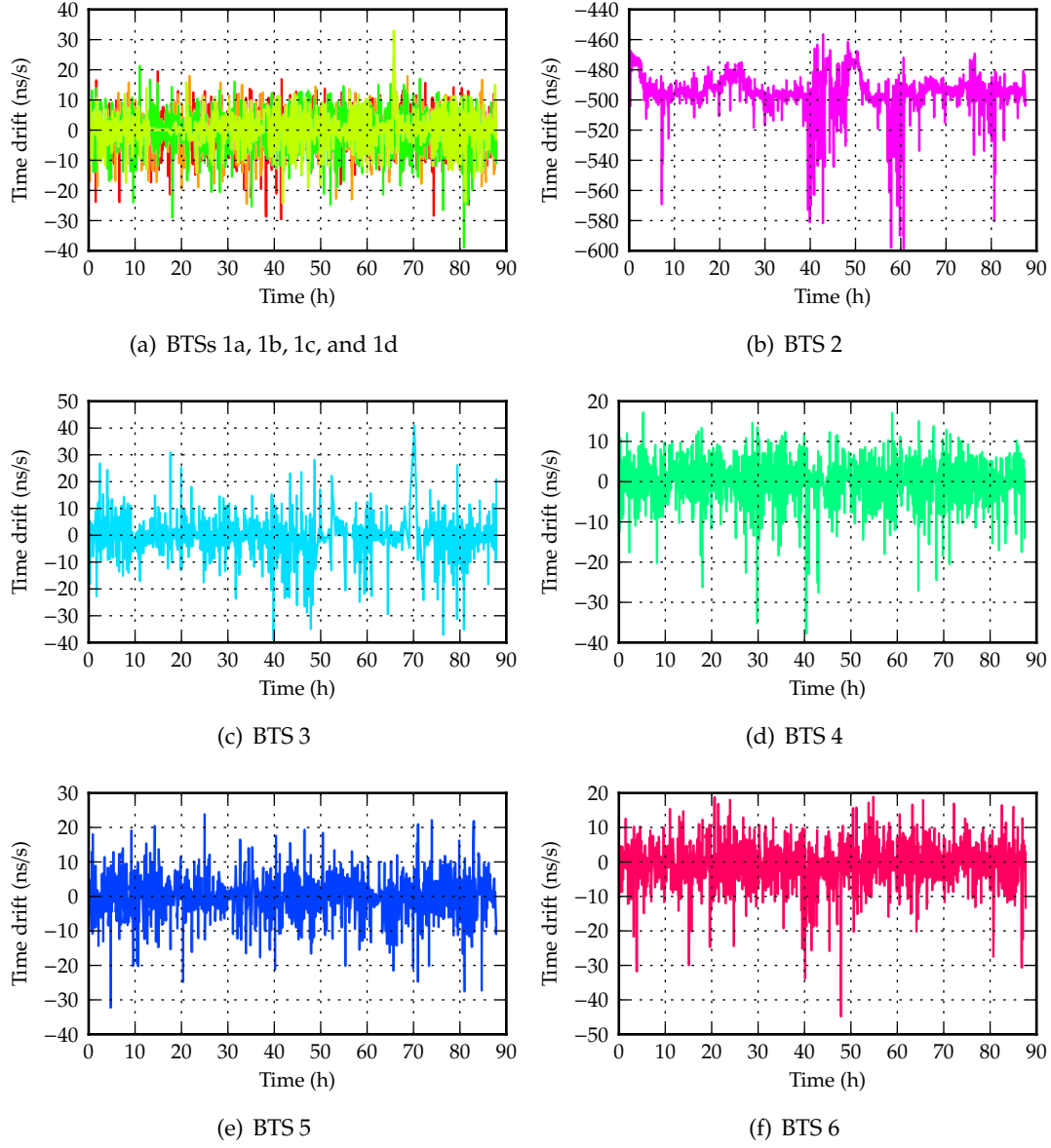


Figure 4.3: Drift rates of the BTS clocks estimated from the synchronisation bursts. Results have been smoothed.

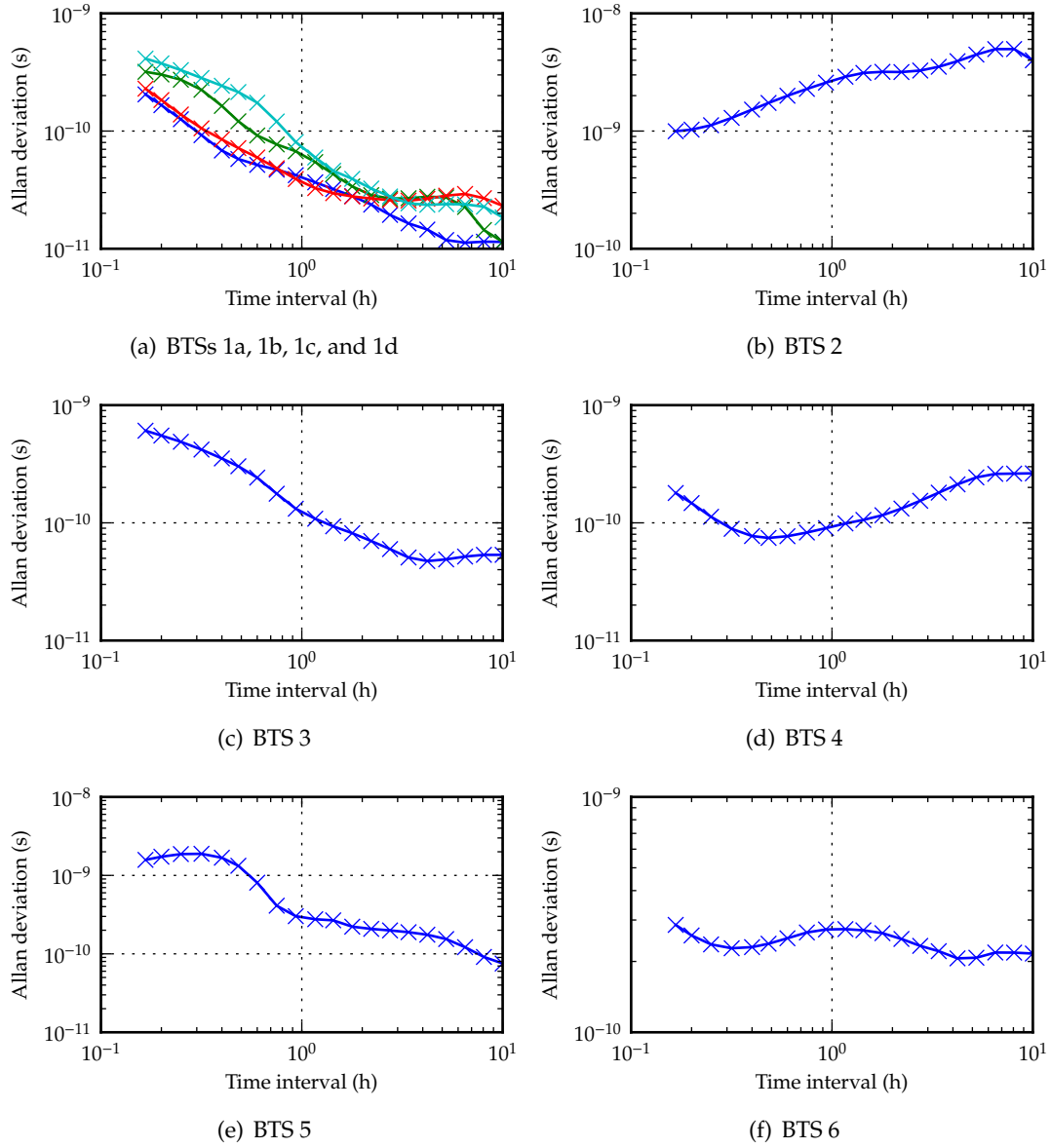


Figure 4.4: Allan standard deviations of the times of arrival of the synchronisation bursts.

Table 4.3: Time offsets and drift rates of the synchronisation bursts.

BTS	Time offset (s)	Average drift rate (ns/s)
1a	7741.826	-0.01
1b	10 554.790	-0.01
1c	10 125.746	0.00
1d	11 501.398	0.00
2	3064.425	-491.30
3	11 345.324	0.08
4	6962.260	0.25
5	6972.263	-0.02
6	2943.406	0.00

Figure 4.2 shows the estimated times of transmissions of the synchronisation bursts. The TOT, in this case, was a direct indication of the time stability of the clocks because the receiver was static. Some of the base stations were not in the line-of-sight of the receiving antenna, although the effects of multipath are too small to be visible at the scale of the figure.

We note there is no general behaviour of the time deviations shown in Figure 4.2. The plots of the estimated drift rates, in Figure 4.3, are noisy but do not suggest any common behaviour of the drift rates either. I did not want to increase the level of filtering of the drift rate estimates to avoid smoothing too much the results and hiding short-term instabilities. BTSs 1a, 1b, 1c, 1d, and 3 are the most stable and their time deviations evoke the random-walk behaviour of a free-running oscillator. On closer examination, BTS 1d shows some rapid oscillations that may indicate a system is controlling the oscillator. It is possible that the sampling period of the measurement is too slow to highlight the operation of a feedback mechanism on BTSs 1a-d. Besides, the Allan standard deviation of BTSs 1a-d indicates a stability better than 1×10^{-10} over 10 hours. The maximum observation period of the plot of the sample Allan standard deviation is limited to about 10 hours and there is no trend indicating that the long-term oscillator stability worsens for longer observation periods. The good stability properties and the presence of deterministic oscillations suggest the oscillator is not free-running but is disciplined by an external reference oscillator. BTSs 1a-d have a common behaviour and may be controlled by the same mechanism, possibly located at the BSC. I was not able to locate BTSs 1a-d with certainty although a simple triangulation experiment suggested that they were spread between two different sites. Their frequencies are allocated to the same network operator, suggesting that they may share the same BSC or that their equipment is provided by the same manufacturer.

The time deviations of BTS 2, 4, 5, and 6 have sudden changes that can also be evidence of external feedback mechanisms controlling the oscillators. The most striking example is the BTS 5, shown in Figure 4.2(e). The time deviations of that BTS have a regular pattern of seven oscillations of about one-hour period and an amplitude of $10\text{ }\mu\text{s}$, which repeats with a period of about 24 h. This may be caused by the daily calibration of the clock with an external frequency reference. Signals from the other BTSs did not show such periodicity.

The offsets and the drift rates of the synchronisation signals, which are used as observations of the BTS clocks, are shown in Table 4.3, after correction for ageing of the frequency standard. The time offsets presented in Table 4.3 are calculated in reference to the origin of the current hyper-frame and are not corrected for the signal propagation time. We can see that none of the base stations has the same time offset. We might have expected that all the BTS belonging to the same cell or attached to the same BSC had synchronised hyper-frames. This is however not the case; we do not observe any synchronisation of the hyper-frame origins between any base station. It is possible that the feedback mechanisms noticed previously only control the frequencies of the oscillators and that the global synchronisation of the network is never considered.

Therefore, it is likely that all BTS oscillators were disciplined by external mechanisms that provided feedback about the frequency errors of the oscillators. However, as implied by the time offset in Table 4.3, the absolute counters of the clocks did not seem to be synchronised to any common reference.

Figure 4.4 shows the Allan standard deviation of the time of arrival of the synchronisation bursts. The Allan standard deviation is used outside its domain of validity, since most of the time deviations do not seem to come from a free-running oscillator. Nevertheless, it provides some useful information about the long-term stability of each BTS. We can see that the synchronisation signals of most base stations have a stability better than 1 ppb over 10 hours. BTS 2 is the only base station for which even the short term stability is worse than 10 ppb, although it is still within the 50 ppb limit set by the 3GPP standard.

Favey *et al.* (2001) also noted that the BTS clocks were disciplined by a common oscillator. They recorded GSM times-of-arrival for 12 hours and observed a time deviation of less than $10\text{ }\mu\text{s}$ on one network and less than $1.5\text{ }\mu\text{s}$ on another. They showed that a feedback mechanism was operating on one network by inserting time step changes of about $0.92\text{ }\mu\text{s}$, which corresponds to the quarter of a GSM symbol period.

4.5 Prediction of time deviations

The time stabilities of the synchronisation bursts are not what we would expect of free running oscillators. Feedback mechanisms introduce large changes at random times. Yet, as we have seen in the previous section, the long-term time stabilities of the base station oscillators are better than 1 ppb over 24 hours in most circumstances. The aim of this section is to evaluate whether a simple filter, based on a model of a free-running oscillator, can predict the time deviations from measurements taken several hours beforehand. I reused the measurements from the experiment presented in Section 4.4.

System model and oscillator parameters

Most base stations, with the exclusion of BTSs 1a-1d, are not free-running oscillators and thus cannot be modelled using simple linear models with Gaussian statistics. Nevertheless, I investigated the prediction performance of a linear Kalman filter with such models.

I assume that the measurement model includes an additive white Gaussian noise. This noise model may not be strictly accurate and Faragher *et al.* (2010) found that the distribution of the TOA error was better described by a Cauchy distribution than a Gaussian distribution. However, the Gaussian noise assumption provided a good starting point for the analysis. I investigated two possible values for the standard deviation of the noise: a fixed value and the maximum-likelihood estimate based on the measurements. The fixed standard deviation of the measurement noise, σ_z , was set to 0.5 μs , or about 150 m, as measured by Faragher (2007). The maximum likelihood estimate of the measurement noise is described in the next section.

I considered two types of oscillator process models. I first modelled the oscillator using the two-state model described by Equation 4.1. The filter thus tracked the time deviation, $b_i(t)$, and the drift rate, $\dot{b}_i(t)$, of each base station i . I also considered the simpler and more generic model of a random walk, where only the time deviations $b_i(t)$ were tracked.

The maximum-likelihood estimates of the h -parameters were calculated by numerical optimization of the log-likelihood function of the Kalman filter, as described in Chapter 2.10. This was in an off-line method, which was applied only after a large number of samples had been collected. The filter was then run again with the previous measurements and with the optimised covariance matrix. On-line methods, for instance the adaptive Kalman filter introduced by Mehra (1970), are also possible: they perform both the state estimation and the covariance parameter optimisation using all the

measurements made. I chose off-line estimation for its simplicity and because it was closer to what a practical system would deploy. Such a system may include a network server to collect information from several devices and perform the optimisation. Updated oscillator parameters are then communicated to the devices, thus avoiding the need for the device to perform a computationally-demanding operation. If network communication is not available, the device may use an on-line method, with degraded performance.

Typical h -parameters lie in the range of 10^{-30} to 10^{-10} and they are scale parameters for the likelihood function. I improved the conditioning of the optimisation problem by using the logarithm of the h -parameters, rescaled and shifted to fit the appropriate range of the optimisation algorithm. I used the Broyden-Fletcher-Goldfarb-Shanno (BFGS) algorithm provided by the Scipy library (see Jones *et al.*, 2001) to perform the numerical optimisation. The values of the maximum-likelihood parameters are shown in Table 4.4 with an optimised measurement noise.

We can look at the optimised h_{-2} parameters to analyse the long-term stabilities of the signals. The signals from base stations 1a-1d are the most stable and those from BTS 2 are the least stable, regardless of the optimisation of the measurement noise. Signals from BTS 3 have the second best long-term stabilities when the measurement noise is optimised (in Table 4.4), but signals from BTS 5 and 6 have better stabilities when the measurement noise is fixed. BTS 3 is the only BTS with an estimate of the measurement noise larger than $0.2 \mu\text{s}$ of standard deviation and it is $0.07 \mu\text{s}$ larger than the second-largest measurement noise. We can corroborate these estimates by observing that the measurements in Figure 4.2(c) are noisier than the others. The reasons for a large measurement noise are probably a weaker signal strength and a more important multipath propagation for this BTS.

Table 4.4: Maximum-likelihood h -parameters of the process model and of the standard deviation of the measurement noise σ_z

BTS	σ_z (μs)	h_0 (s)	h_{-2} (s^{-1})
1a	0.15	1.6×10^{-17}	4.3×10^{-30}
1b	0.13	9.1×10^{-17}	8.9×10^{-32}
1c	0.16	3.4×10^{-17}	3.1×10^{-32}
1d	0.16	1.2×10^{-16}	2.0×10^{-32}
2	0.11	6.6×10^{-15}	2.6×10^{-15}
3	0.25	4.0×10^{-16}	3.5×10^{-28}
4	0.12	4.1×10^{-17}	2.0×10^{-25}
5	0.15	3.0×10^{-22}	4.1×10^{-22}
6	0.14	9.6×10^{-17}	1.2×10^{-24}

The model can be checked using the normed innovation squared (NIS) of the Kalman filter, which was introduced in Section 2.1. The NIS follows a χ^2 distribution with two degrees of freedom if the filter is properly “tuned” to produce an optimal estimate from the measurements. The NIS is not a universal measure of the goodness-of-fit of the model to the process being studied. More advanced methods may be required to compare different models. However, the NIS provides a useful and simple way to check the goodness-of-fit of the process and measurements models by comparing the sample distribution of the NIS with its theoretical distribution. We visualise the comparison between the sample and the theoretical distributions on probability plots, also called Q-Q plots.

Figure 4.5 shows the probability plots of the NIS when the model parameters are tuned to a random-walk model and Figure 4.6 shows the probability plots of the NIS for a the two-state oscillator model. There is generally a good agreement between the theoretical and observed distributions of the NIS for both models, except for BTS 2. This is expected since we saw in Section 4.4 that the timing signals from BTS 2 have the largest dynamics and seem to be derived from a disciplined clock with large corrections. There is no significant difference between the one-state and two-state models. The NIS tends to be biased in different directions for BTS 4, which may result in different errors. The oscillations observed in the signals from BTS 5 do not appear on the NIS distributions. This is probably because the diffusion and h -parameters are too large to consider the oscillations as process noise.

I tried an ad-hoc solution which consisted of “artificially” increasing the state covariance matrix every time the NIS crossed a threshold, for example six times the normal standard deviation. This technique is sometimes called *innovation gating* in the Kalman filter literature. However, this method did not significantly improve the prediction performance. The prediction interval may have included more than one step change of the frequency drift, which could not have been modelled by simply increasing the process covariance. The control mechanisms that introduced the large frequency drift variations appeared to be triggered at random times, which hindered long-term predictions. Even more sophisticated approaches, such as the interacting Markov model Kalman (IMM) filter (Blom *et al.*, 1988) or the switching Kalman filter (Murphy, 1998), may not have improved the prediction performance because the process that created the frequency drift variations could not be modelled accurately.

The results are shown with a maximum-likelihood estimate of the measurement noise variance. The measurement noise depends on the position of the user and thus can not be known or distributed in a practical system. I thus chose a constant

and conservative value of the measurement noise variance in the rest of this chapter, compatible with the existing literature about the measurement noise of propagation times in urban environments, and I chose $\sigma_z = 0.5 \mu\text{s}$.

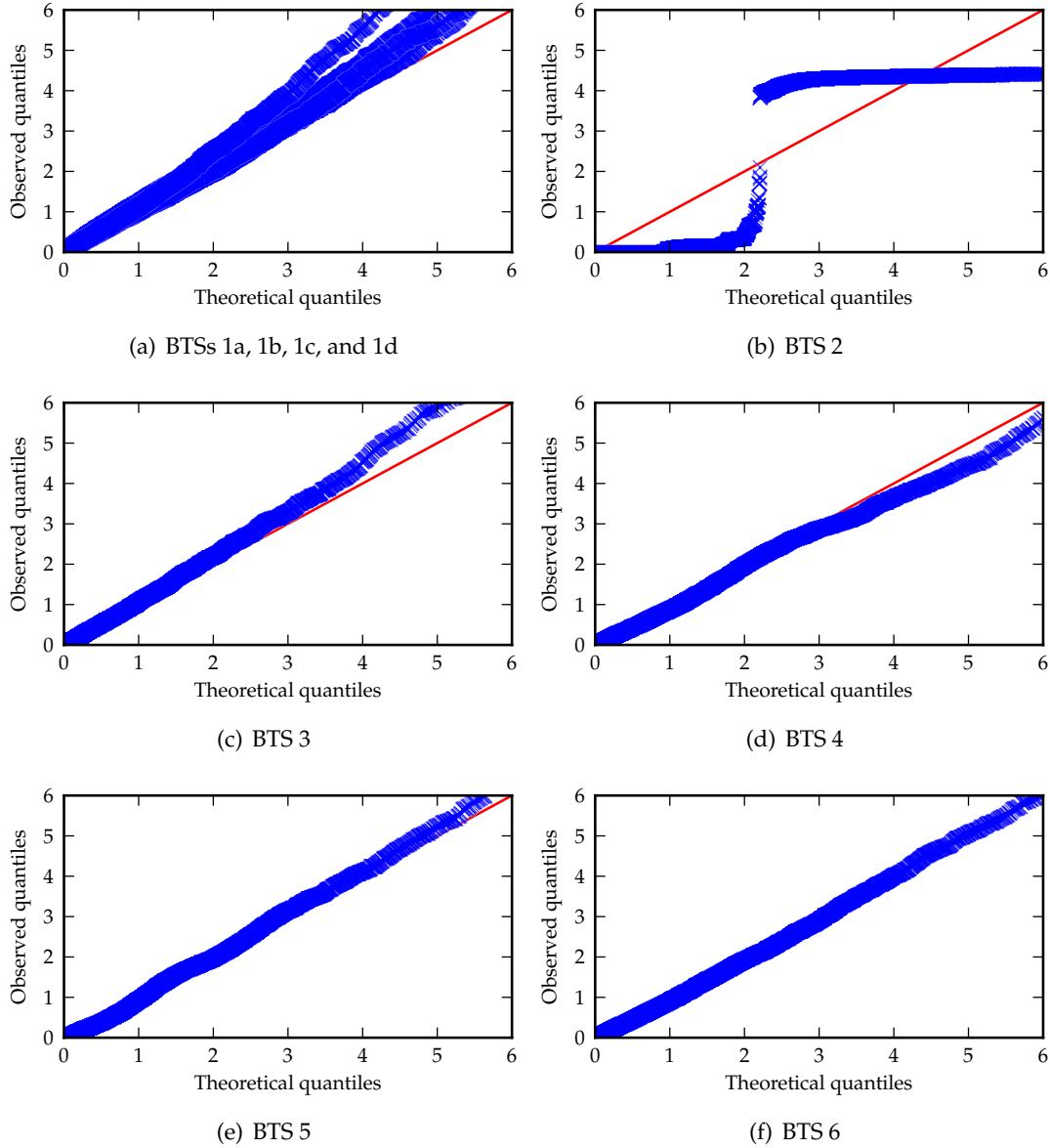


Figure 4.5: Q-Q plots of the normalised innovation squared of the Kalman filter with the one-state model.

Time prediction

I predicted the time deviations of the clocks using the same experiments as the ones presented in Section 4.4. The predictions were performed using the one-state and the

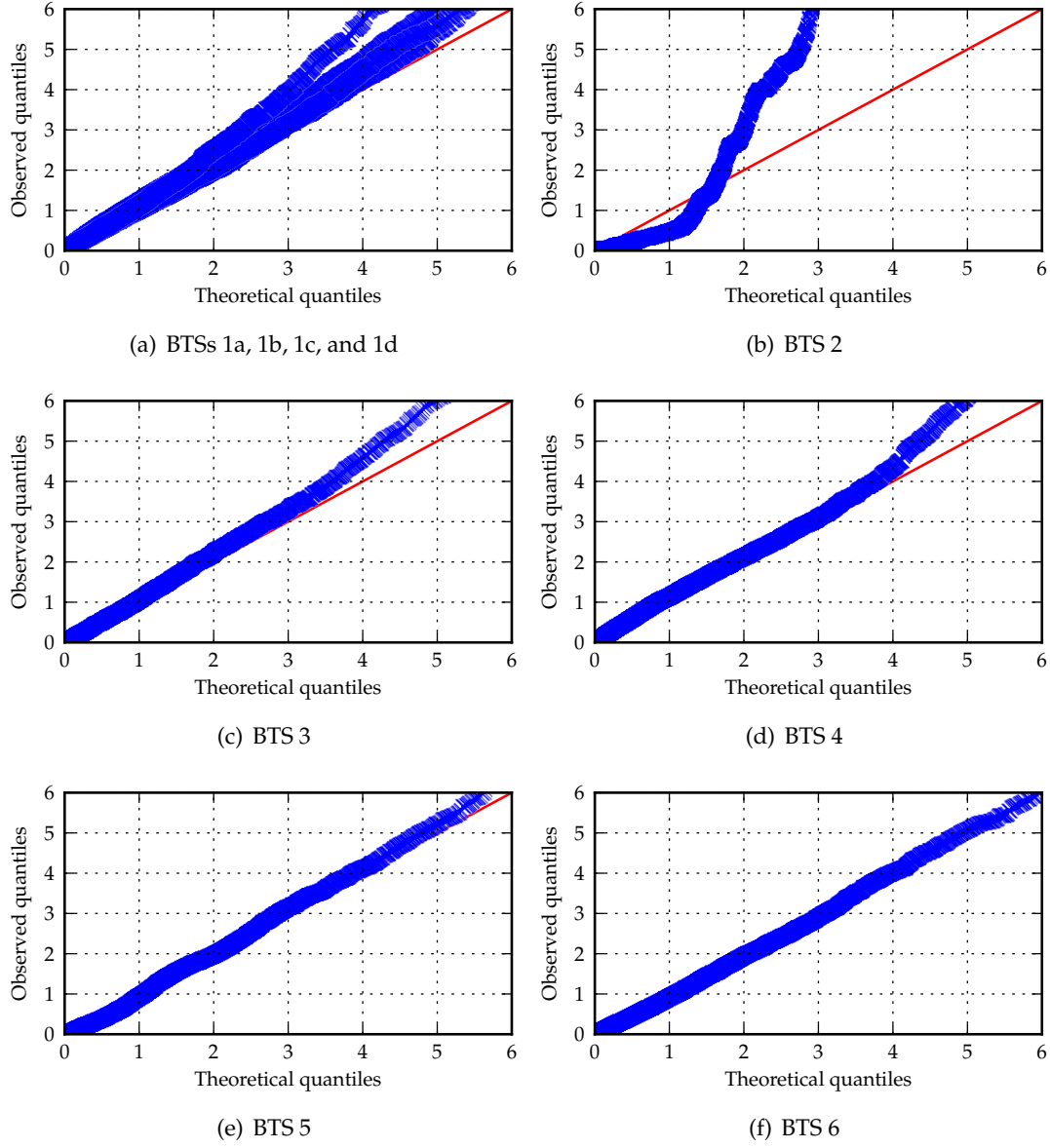


Figure 4.6: Q-Q plots of the normalised innovation squared of the Kalman filter with the two-state model.

two-state linear models of the oscillators, which were tuned to the maximum-likelihood parameters calculated in the previous section. A Kalman filter was used to estimate the time deviations at a given time and then to propagate the state to predict the time deviations at a future time. The prediction interval was varied between one and twenty-four hours and the GPS time was observed for about ten minutes at every update. The filter was initialised with an estimate of the clock offset and drift rate from the first 100 measurements. I then calculated the errors between the predicted values and a linear interpolation of the nearest measurements.

The prediction errors using the one-state oscillator model are shown in Figure 4.7. The one-state model is a random walk, hence it can not track the frequency drift of an oscillator. The prediction step consists of simply reporting the current time deviations at a future time. This method is similar to assuming a constant error in the time deviations, which could be done with a solution simpler than a Kalman filter. However, the Kalman filter may reduce the prediction error since it may improve the estimation of the current time deviations. These time deviations can be predicted with errors better than $50\text{ }\mu\text{s}$ for all base stations, except BTS 2. BTS 4 has the second-worst prediction performance and it has a prediction error bias of about $30\text{ }\mu\text{s}$ for prediction intervals longer than 12 h. The normalised innovation squared of the model, shown in Figure 4.5, suggests the model is biased when using the measurements from BTS 4. A similar bias is observed in the NIS plots and the prediction errors of BTSs 1a-d and 3, although the magnitudes of the biases are smaller than for BTS 4. BTS 4 has the largest amplitudes of the time fluctuations of all the BTSs except BTS 2, as shown in Figure 4.2, hence it has the largest bias, since the one-state model simply propagates the current time deviation.

The results using the two-state oscillator model are shown in Figure 4.8. The time prediction errors are generally worse than in the case of the one-state model. It is interesting to note that the NIS plots, in Figure 4.6, do not suggest such a large difference between the one-state and two-state models.

The time prediction errors are mostly caused by changes in the clock drift rates, probably triggered by control feedback mechanisms. The two-state oscillator model does not bring any advantage over the simple random-walk model, which in fact gives the smallest prediction errors. Tracking the drift rate component of the oscillator, as done in the two-state model, is not worthwhile when considering controlled oscillators. The dynamic linear model assumes that the frequency drift follows a random walk, although a disciplined oscillator generally controls the frequency with discrete step changes. We could improve the filter by adding a discrete state variable, which estimates if the clock is in feedback mode, although such a model seems impossible to design

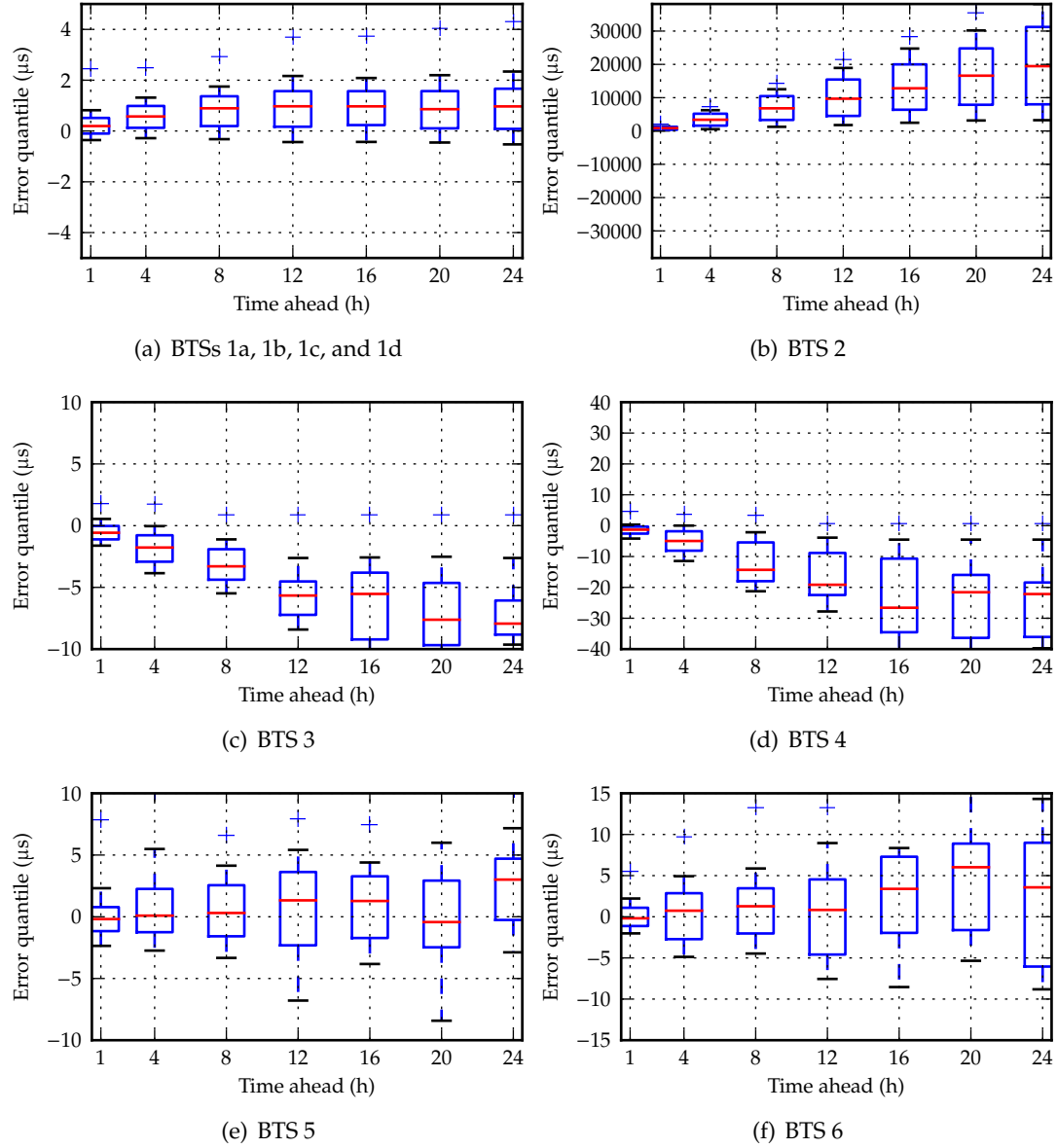


Figure 4.7: Box-plot of the prediction errors of the GSM time signals, using a one-state oscillator model (random walk model). The red horizontal line is the median value; the blue central rectangle extends from the 25-percentile to 75-percentile; the black horizontal lines mark the 10-percentile and 90-percentile; and the blue crosses indicate the maximum and minimum values.

because the control mechanism does not seem to follow any predictable law.

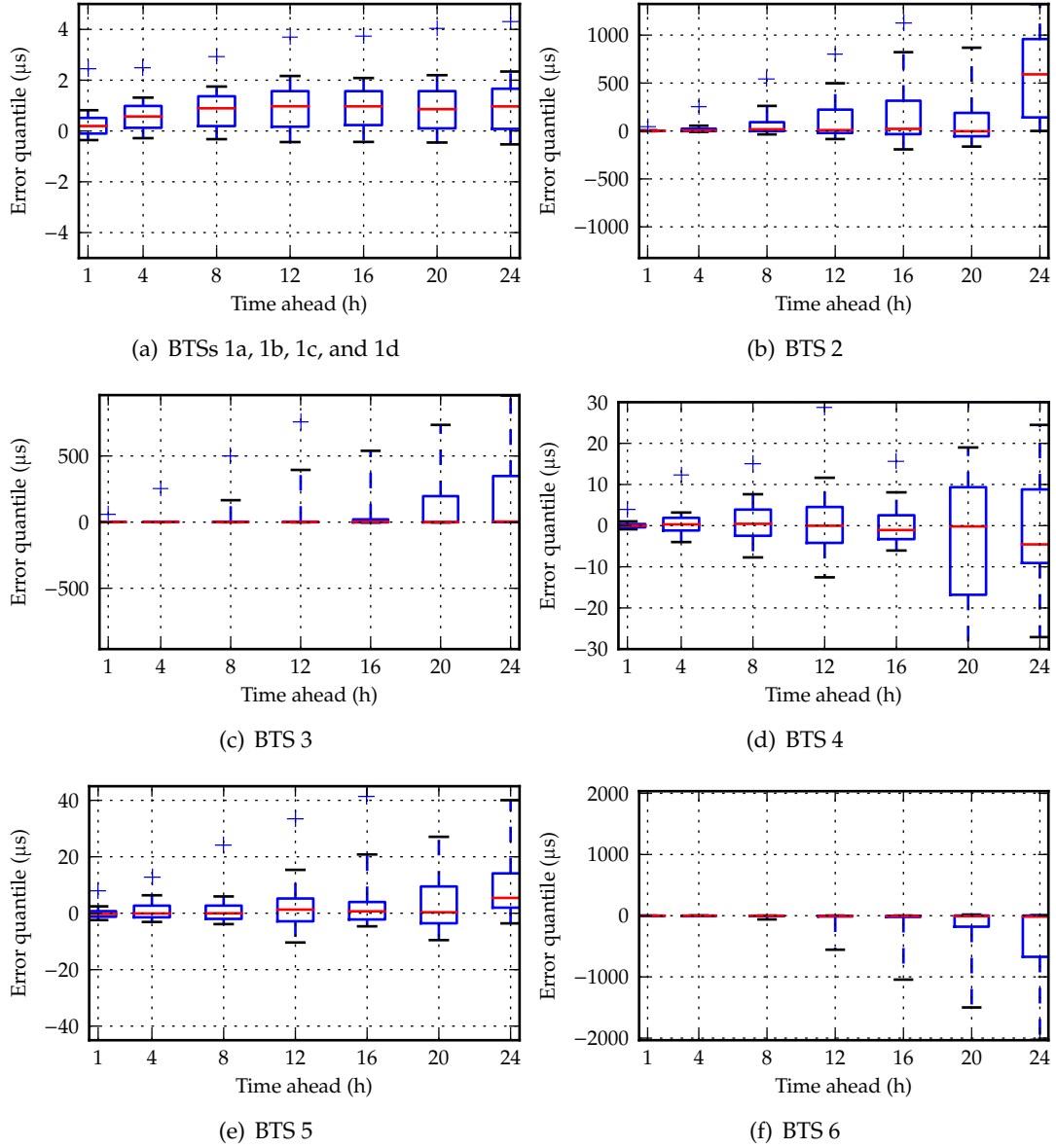


Figure 4.8: Box-plot of the prediction errors of the GSM time signals, using a two-state oscillator model.

4.6 Tracking of local oscillator bias

We now exploit the long-term stability of the BTS clocks to correct the time offset of the local oscillator of a mobile device. We consider a practical application similar to the one described in the previous section: a mobile device tracks the time deviations of several reference clocks with the goal to provide fine-time assistance to a GPS receiver, thus improving the TTFF. In the previous section, we considered the time deviations of the BTS clocks individually and we did not use the short-term stability of the local

oscillator. This model is now improved by building a *clock ensemble*, which contains all the clocks in the system, including the local oscillator.

Ensemble clock filter

Time is measured by a clock whose process is inherently noisy. We can filter the observations from a clock to improve the time estimate if the noise characteristics are known, as was done in the previous section. We can also improve the time estimation by combining the measurements from several clocks, since the noise processes are generally uncorrelated between different clocks. A filter typically keeps track of the time fluctuations of each clock with respect to a common time reference. A better estimate of the time reference is then obtained by a weighted average of the filter estimates.

The case of UTC raises specific problems since the goal is to define a stable time scale and not simply to track the deviations of several clocks. The UTC time scale is estimated by an ensemble of atomic clocks from several laboratories. This system is not fully observable: the time scale is undetermined and only time differences between the atomic clocks are observed. This leads to convergence issues with the ensemble filter and Galleani *et al.* (2003) reviewed some of the possible solutions. The same problem occurred when the GPS time scale was established. An early approach relied on a master clock, which served as the reference time of all time observations. The GPS composite clock, presented by Brown (1991), was then developed to build an independent time scale. However, we do not have such a problem when estimating the local time. All the time measurements in a mobile receiver have a common time scale and the clock ensemble considered in this section is thus fully observable. The time deviations of all the clocks are measured with respect to the GPS composite clock given by the GPS software receiver, albeit with measurement errors.

I evaluated the performance of the ensemble filter for the two process models presented in Section 4.3. I only describe the equations of the clock ensemble filter for the two-state oscillator model, as the equations of the random-walk model are straightforward to derive. The state vector of the clock ensemble with the two-state process model is

$$\mathbf{x}(t) = \begin{bmatrix} b_{\text{local}}(t) & \dot{b}_{\text{local}}(t) & b_1(t) & \dot{b}_1(t) & \cdots & b_N(t) & \dot{b}_N(t) \end{bmatrix}^T,$$

where $b_{\text{local}}(t)$ is the time deviation of the local oscillator and $b_{1..N}(t)$ are the time deviations of the synchronisation bursts from the base stations. All times are in the GPS

system time scale. The state vector is estimated by a Kalman filter and the estimate is a Gaussian random variable with mean $\hat{\mathbf{x}}(t)$ and covariance matrix $\mathbf{P}(t)$.

The time of transmission of the synchronisation bursts from base station i , received at time t in the receiver time scale, is noted $t_i^{(GSM)}(t)$. The GPS time, calculated at time t in the receiver time scale, is noted $t^{(GPS)}(t)$. The relationships between these time measurements and the components of the state vector are given by

$$\begin{aligned} b_{\text{local}}(t) &= t - t^{(GPS)}(t) \\ b_i(t) &= t_i^{(GSM)}(t) - t^{(GPS)}(t) \quad \text{for } i = 1 \dots N. \end{aligned}$$

There are two measurement models, depending on whether a GPS measurement is available or not. Most of the time, the filter tracks the time deviations of the BTS clocks using the times of arrival of the synchronisation bursts. These measurements are performed in the local time scale of the receiver whereas the state vector is expressed in the GPS time scale. The difference between the local and the GPS time scales are not known until a GPS measurement is made, hence the system is not fully observable using the GSM timing signals only. If a GPS observation is available, the time deviations can be directly observed

$$\mathbf{z}_i(t) = \begin{bmatrix} b_{\text{local}}(t) & b_i(t) \end{bmatrix}^T + \mathbf{R} \mathbf{w}(t),$$

with the corresponding observation matrix being a $2 \times 2N$ matrix and $H_{0,0} = 1$, $H_{1,2i} = 1$, and all the other elements set to 0. The observation noise covariance matrix is

$$\mathbf{R} = \begin{bmatrix} \sigma_{\text{GPS}}^2 & 0 \\ 0 & \sigma_{\text{GSM}}^2 + \sigma_{\text{GPS}'}^2 \end{bmatrix}.$$

where σ_{GSM} and σ_{GPS} are the standard deviations of the GSM and GPS measurement noises, respectively.

If a GPS measurement is not available, the time deviation of the BTS i is measured with respect to the local oscillator and the measurement equation becomes

$$\begin{aligned} \mathbf{z}_i(t) &= \begin{bmatrix} t_i^{(GSM)}(t) - t \end{bmatrix}^T + \mathbf{R} \mathbf{w}(t) \\ &= \begin{bmatrix} b_i(t) - b_{\text{local}}(t) \end{bmatrix}^T + \mathbf{R} \mathbf{w}(t). \end{aligned}$$

The corresponding observation matrix is a $1 \times 2N$ matrix with $\mathbf{H}_{0,0} = -1$, $\mathbf{H}_{0,2i} = 1$, and all the other elements set to 0. The observation noise covariance matrix is simply $\mathbf{R} = \begin{bmatrix} \sigma_{\text{GSM}}^2 \end{bmatrix}$.

We remark that the observation time, t , is both a measurement and a variable of the process model. We assumed a noise-free measurement of the local time, although

in theory there may be some noise if the triggering of the GSM or GPS measurements is not perfectly synchronised with the local clock. In practice, I did not observe such problems.

Local oscillator tracking experiment

The experiment is representative of a mobile device with a low-cost local oscillator and with access to both GPS and GSM signals. The goal is to track the time bias of the device's clock in order to provide fine-time aiding to a GPS receiver, whenever the user needs it. At periodic intervals, the mobile device performs a GPS acquisition and calculates its position and the bias of its local clock in reference to the GPS time. The device also receives the synchronisation signals from the GSM base stations and feeds them to a clock ensemble filter. The latter, provided with a model of the BTS oscillators and the local clock instabilities, keeps an estimate of the local clock bias between the GPS updates. The GSM base stations provide time measurements that have worse stabilities and accuracies than the time derived from GPS signals, but they are typically stronger than GPS signals and can be acquired indoors.

The experimental arrangement, outlined in Figure 4.1, was similar to the one used for the experiment presented in Section 4.4. The only change was the source of the triggering signal, which was derived from a mass-market Quartz crystal oscillator instead of the more-accurate atomic frequency reference standard. The trigger signal was used both as the local clock and as the signal that synchronised the time measurements. This arrangement highlighted that the sampling rate did not have to be constant. The sampling instant t was only required to synchronise the measurements of the local clock, $t^{(local)}(t)$, and the GSM time signals, $t^{(GSM)}(t)$. The role of the local oscillator of the mobile device was performed by the crystal oscillator embedded in the digital counter card. Its performance was unknown and the datasheet only mentioned its frequency accuracy, of 50 ppm over the temperature range of -20°C to 70°C . I opened the acquisition board and identified the oscillator as a Pletronics CMOS Quartz crystal oscillator, without temperature compensation.

The GPS signal was recorded only once per hour to limit the storage space requirements. We can determine the time bias of the local clock accurately only during these GPS measurements, which is not problematic for the filter operation since the drift rate is estimated over long observation periods. However, the filter performance was evaluated by calculating the error between the estimated time bias and the observed time bias, which was available only during the GPS measurements. We thus need an accurate estimation of the local time bias at a higher rate than the GPS updates in

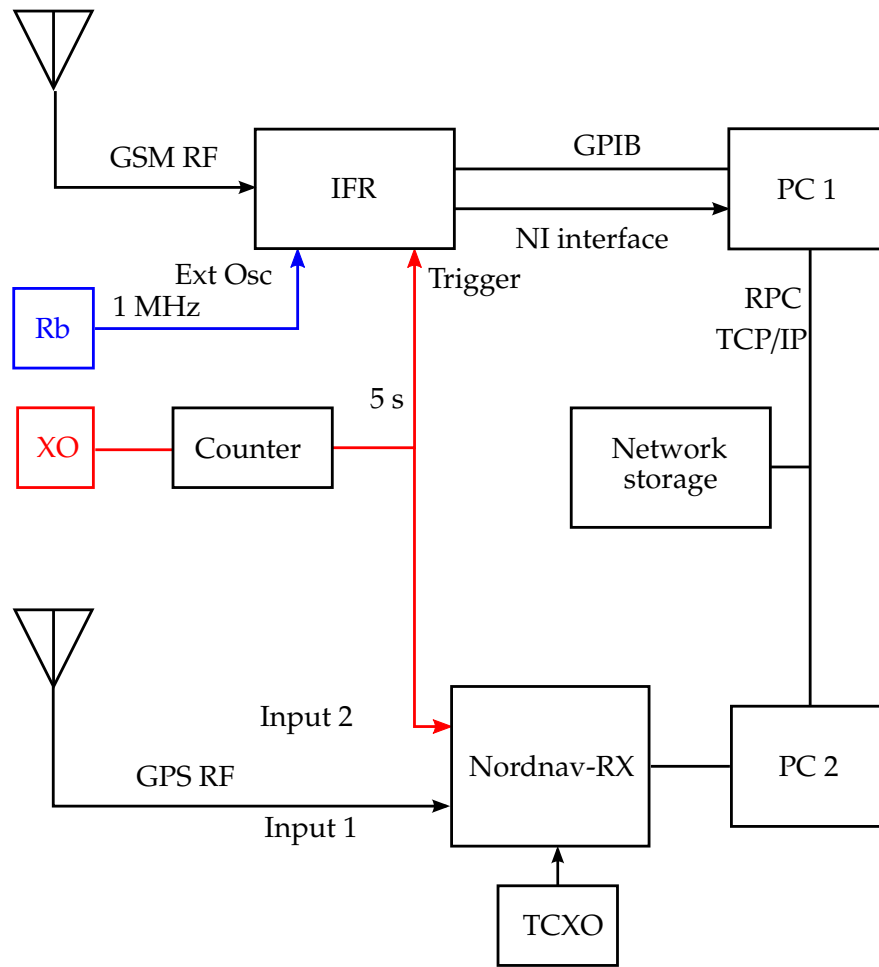


Figure 4.9: Schematic diagram of the experimental arrangement using a Quartz oscillator. The diagram does not represent the real physical location of the components.

order to evaluate the tracking performance of the filter for every GSM measurement. I interpolated the bias of the local clock between the GPS measurement periods. I first tried classical interpolation functions, such as the linear and spline models, but these methods created a large tracking error of the filter between the interpolation points, at the GPS update times. I considered that the origin of these errors was not physical but in fact a poor fit of the interpolation functions. I suspect that the random-walk behaviour of an oscillator cannot be modelled with enough accuracy by interpolation functions with such low polynomial orders. A Gaussian process regression, as described by Rasmussen (2006, chapter 2), resulted in smaller residual errors than the other interpolation methods. I therefore used a Gaussian process, with a squared-exponential covariance matrix of characteristic length four hours, in order to

provide the time bias of the local clock with respect to the GPS time.

The ensemble filter was initialised with the average bias and the average drift rate of each clock, estimated over the first three hours of data collection. In a practical application, the filter could be initialised from estimates kept in a central database or transmitted from nearby devices. The process covariances of the BTS clocks were set to their maximum-likelihood estimates, calculated in Section 4.5.

Most mobile devices already keep an estimate of the current ageing of the local oscillator but do not optimise the noise covariance parameters. We could calculate the maximum-likelihood parameters of the local clock from the less noisy GPS time measurements. However, it is necessary to keep a history of all previous measurements to run the filter, which may not be practical in a real application. Instead, I tried a few combinations of h -parameters within two orders of magnitude of the parameters of a typical low-quality oscillator. I kept the parameters that gave the smallest tracking error: $h_0 = 10^{-16}$ and $h_{-2} = 10^{-17}$.

I set the cross-covariance terms to zeros, thus making the assumption there was no correlation between any two clocks of the ensemble. This is not entirely correct since we expect that some BTSs are connected to a common clock reference and that local propagation effects may introduce some correlation between the signals arrival times. I also ran the filter with the cross-correlation terms set to the sample cross-covariance calculated from the measurements taken in Section 4.4 and the changes in the results were less than 1 μ s.

GPS-aiding of the local oscillator

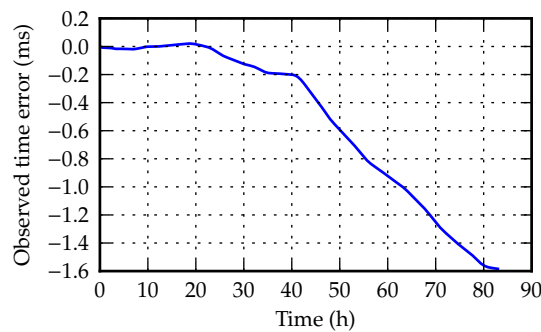


Figure 4.10: Time bias of the local clock, recovered from GPS time measurements.

Figure 4.10 shows the error in the time calculated by the local clock, using the GPS interpolation as true time.

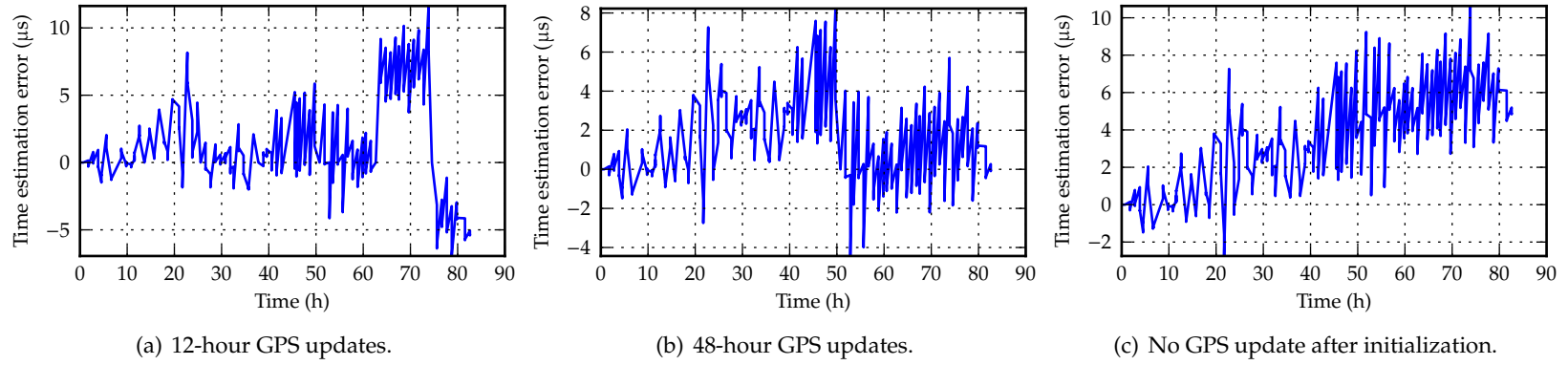


Figure 4.11: Time series of the local time error after filtering, all base stations, one-state model.

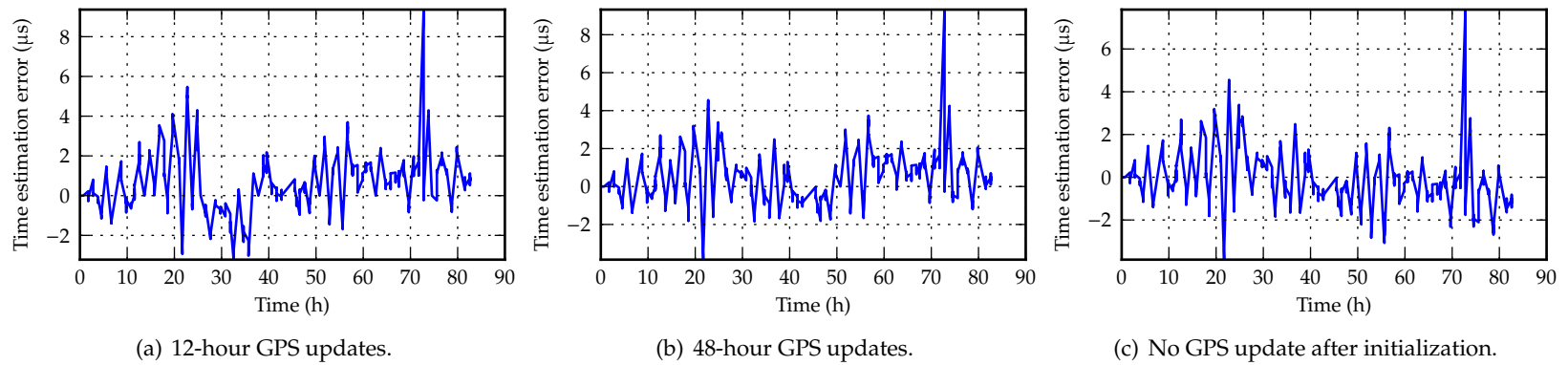


Figure 4.12: Time series of the local time error after filtering, all base stations, two-state model.

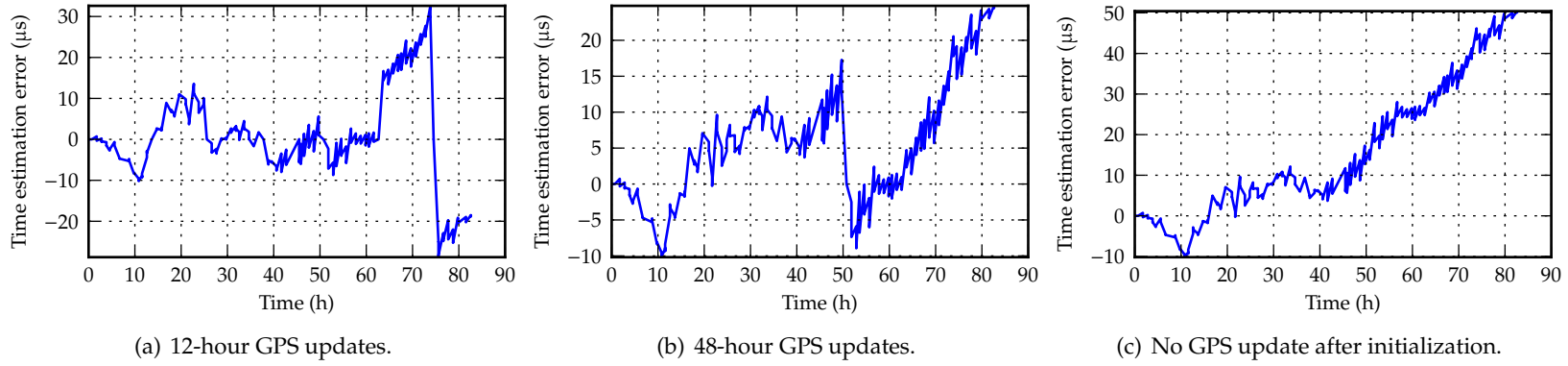


Figure 4.13: Time series of the local time error after filtering, least stable base stations, one-state model.

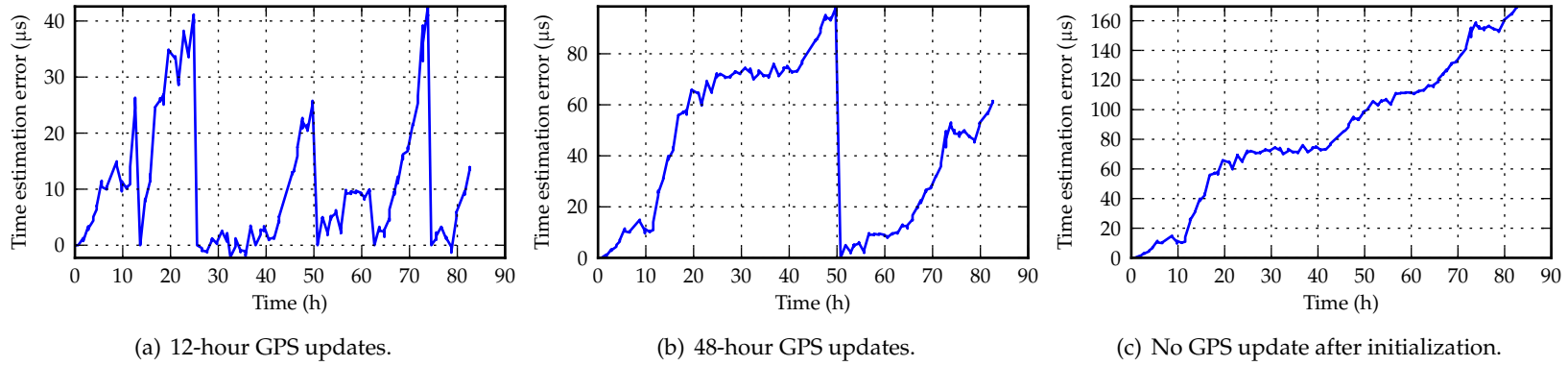


Figure 4.14: Time series of the local time error after filtering, least stable base stations, two-state model.

I analysed the results in four different scenarios. I first ran the filter with the measurements from all the nine BTSs available. The tracking errors are reported in Figure 4.11 for the one-state model and in Figure 4.12 for the two-state model.

We are also interested in the performance of the filter in absence of stable BTS signals. I ran the filter again with all the measurements except those from BTSs 1a to 1d and BTS 3, which were the most stable BTSs. This was to test the behaviour of the filter when accurate measurements were not included in the ensemble. The tracking errors are shown in Figure 4.13 with the one-state model and in Figure 4.14 with the two-state oscillator model.

As expected, the performance varied depending on the stabilities of the signals and on the number of states in the process models. The two-state model performed slightly better than the one-state model when the signals from all BTSs were included. The maximum time error with a two-state model, shown in Figure 4.12, was about $8\text{ }\mu\text{s}$ and the median time error was under $1.2\text{ }\mu\text{s}$, for all GPS update periods. The maximum error with a one-state model was $10\text{ }\mu\text{s}$ and the median error remained about the same, except with no GPS update where the median error of the one-state model was about $3\text{ }\mu\text{s}$.

The absence of the most stable BTS signals showed a different picture, illustrated in Figures 4.13 and 4.14. The results were significantly worse than when all the BTSs were included. This was expected since the ensemble filter weighed the time measurements according to their time stabilities. The lack of stable measurements affected the estimate of the ensemble, as the weights of the different sources of measurements were now approximately similar. The two-state model performed significantly worse. The two-state filter wrongly estimated the drift rate of some of the BTS signals, leading to an increasing time error that reached more than $70\text{ }\mu\text{s}$ after 24 h. The maximum error, without any GPS update, was about $160\text{ }\mu\text{s}$ after three and a half days. It is interesting to note that the estimation error was always positive, which may be explained by a bias in the initial drift rate estimate. However, even a time accuracy of $160\text{ }\mu\text{s}$ can benefit a GPS L1 C/A receiver, whose code period is 1 ms.

4.7 Discussion and conclusions

GPS time estimation using fractional pseudo-ranges

The software receiver I used to calculate the GPS time in this chapter extracts the full pseudo-range measurements of the GPS signals; however, most of the receivers found in mobile devices only use fractional pseudo-ranges, as explained in Section 2.5. The

time ambiguity of fractional pseudo-range measurements is an integer number of the PN code period. Syrjärinne (2000) compared simulations and experimental results of the recovery of GPS time from a millisecond-ambiguity algorithm. He concluded that the GPS time could be accurately recovered under strong signal conditions and a good constellation geometry. However, the time error may be too large for sub-millisecond accuracy in degraded situations. His simulation results showed that the GPS time could be calculated with an accuracy of 3 ms, with an integer ambiguity of 1 ms. The results he obtained from a GPS receiver connected to a GPS simulator were significantly less accurate, with errors up to 50 ms in poor constellation geometry and the millisecond ambiguity was not evident.

Recovering the GPS time from fractional measurements is difficult because the times of transmission of the GNSS signals are unknown and need to be estimated by the algorithm. A receiver that decodes the navigation signals can accurately determine the TOT from the time-of-week word in the navigation message. Otherwise, algorithms based on fractional measurements must estimate the TOT, as explained in Section 2.5. An error in the estimation of the time of transmission results in an error in the GPS time estimate and in the user position. A position error ϵ_r introduces a TOT error of ϵ_r/\dot{r} , where \dot{r} is the radial velocity, also called range rate, of the satellite seen from the user position. The timing error, ϵ_t , is proportional to the propagation speed of the signal, which is approximately c . We therefore have $\epsilon_t = \epsilon_r/\dot{r}$. GPS satellites have radial velocities of at most 600 m/s and the pseudo-range measurement errors are typically 30 m. The error in the GPS time estimation is thus about 50 ms in an assisted-GPS receiver.

Assisted-GNSS receivers can thus have difficulties in estimating accurately the local clock bias. This inaccuracy is not critical in mass-market receivers, since the user is often only interested in its position. However, the clock ensemble filter we analysed in this chapter requires accurate time measurements in order to provide an estimate of the GPS system time with a sub-millisecond accuracy. I suspect that the estimation of GPS time from fractional measurements is a problem only during the initialisation of the ensemble filter. The iterative algorithms used to solve the position and time equations are generally sensitive to the starting point, as highlighted by Syrjärinne (2000). I expect the time errors to be negligible when fine-time aiding is available to initialise the iterative algorithm with an uncertainty smaller than the PN code period.

An alternative method would be to make fractional measurements whose time ambiguity is large, hence resulting in a smaller risk of large errors. Akopian *et al.* (2009) propose the detection of the bit edges of the navigation signal, which has a period of

20 ms. The accuracy of the time, using simulated measurements, is negligible though an integer ambiguity of 20 ms can appear at C/N_0 lower than 30 dB-Hz. The new GNSS signals have longer code periods, which improves the errors introduced by the time ambiguities.

Receiver motion

All the experiments were performed with a static receiving antenna. The filter presented in this section can not estimate the GPS system time if the receiver is moving, since it can not distinguish whether the changes in the reception times of the bursts are caused by changes in the transmission times or in the propagation times. Put differently, all the GSM time measurements have an error caused by the confusion between the time deviation of the oscillator and the motion of the receiver. The filter hence needs to estimate the propagation time of the signals as well as the time deviations of the BTS clocks.

One solution is to include the user position in the clock ensemble. The filter updates the mobile position estimates whenever positioning measurements are available, for example using a GNSS receiver. The propagation times can then be calculated, assuming the positions of the BTSs are known, and removed from the times-of-transmission measurements. However, the goal of the experiments presented in this chapter was to provide precise time when GNSS signals were not available, for example indoors. Indoor positioning is notoriously difficult, but the accuracy required for fine-time aiding is of tens of microseconds, or about 3 km, which can be attained in most situations using Cell-ID or RSS positioning. The maximum range within a GSM cell is typically 15 km, or a maximum time error of 50 μ s, which is acceptable for the purpose of time assistance of a GNSS receiver. In comparison, the maximum drift rate of the local oscillator in the experiment was about 35 μ s/h. Solo Matrix, proposed by Duffett-Smith *et al.* (2004), is a positioning method relying on GSM signals. It assumes short-term stabilities of the base stations and calculates the mobile position using the time difference of arrival of GSM signals whose time offsets have been calibrated. Solo Matrix could be easily improved by an ensemble clock filter to propagate the time offsets of the BTSs, thus enabling a more robust positioning from GSM signals than relying only on the short-term stability of one BTS.

Another solution is to use the timing advance (TA) parameter of the GSM protocol, which is proportional to the range between the mobile and its serving base station. The base stations set the TA parameter to command the mobile stations to introduce a time offset at the beginning of their transmissions. This delay ensures the signals

transmitted by users at different distances arrive within their correct time slots at the serving BTS. The granularity of the TA parameters is of one symbol for the round-trip delay, i.e. about $3.7\text{ }\mu\text{s}$ or a distance of 550 m. The TA is necessary because of the TDMA approach used by GSM; it is always implemented and defined in 3GPP (2003b, TS 05.10). Some CDMA systems may also provide distance information as CDMA systems need to adjust their transmission power in order to limit the near-far effect. The TA, or its CDMA equivalent, is provided only by the serving BTS. The corrections are thus limited to only one base station, which is a problem since the goal of the ensemble filter is to exploit the diversity of the measurements from several base stations. However, the receiver motion can be averaged out by using the measurements from several BTSs, which are assumed to be uniformly distributed around the receiver.

Conclusions

The results presented in Section 4.6 show that the GPS time can be predicted within $30\text{ }\mu\text{s}$ using a single daily GPS measurement, for a static receiver. This stability is better than 1 ppb over 24 hours. Most oscillators, like TCXO, can achieve this level of stability over short periods. However, the long-term stabilities of the BTS synchronisation signals could be used to provide fine-time aiding to a GNSS receiver after a period of sleep. The mobile device tracks the time deviations of the signals from the neighbouring BTSs as long as GNSS time and positions can be calculated. The device can then be turned off and still be able to obtain accurate GPS system time immediately after resuming its operations. There is, however, a possibility of time error if the user has moved. Fine-time aiding reduces the time-to-first-fix, thus providing a better experience to the user and saving battery by limiting the time spent in the power-consuming acquisition stage.

GNSS aiding in synchronised cellular networks

I discussed in the previous chapters the theoretical times-to-first-fix (TTFFs) of assisted-GNSS receivers and how the TTFF can be reduced by providing the approximate GPS time to the receiver. The experimental analysis of various GSM networks in Cambridge, United Kingdom, showed that the time signals of these networks are not synchronised and have variable levels of stabilities. Some networks can provide fine-time aiding whereas others are not stable enough. Besides, the GSM synchronisation signals only carry counters that are not related to the GPS time or any universal time scale. The GPS system time can only be determined after having first calibrated the time origins of the counters.

Synchronised networks, such as, for example, CDMA2000, can provide stable and synchronised time information, which can help improve the TTFF performance of a GNSS receiver. CDMA2000 is a technology of synchronised networks mostly deployed in North America, Latin America, and Asia. The standard specifies that the networks must be synchronised with the GPS system time, which opens new perspectives for improving the GPS performance on mobile personal devices. GPS system time can be recovered accurately from the CDMA2000 signals and then used to reduce the GPS signal acquisition search space, thus improving the TTFF performance. The synchronisation of the signals can also be exploited to perform radio positioning, using either only the CDMA2000 signals or in combination with GPS signals. In this chapter, we investigate how the features of synchronised networks can improve the performance of positioning on mobile devices.

5.1 Introduction

CDMA2000 networks

CDMA2000 is a standard of third-generation cellular networks for personal communications. It is an evolution of IS-95, which is a standard of second-generation networks developed by Qualcomm Inc. under the name cdmaOne[™]. Most of the specifications of cdmaOne[™] are proprietary. CDMA2000 is more accessible to the researcher since it is recognized by the International Telecommunication Union (ITU) and, for the most part, by the 3rd Generation Partnership Project 2. We only address CDMA2000 networks in this chapter. However, the work presented in this chapter may only require the specifications of an IS-95 network.

The air interface of the network is based on code-division multiple access with synchronised transceivers. Furthermore, the standard 3GPP2 (2004a, C.S0002) specifies that the time scale employed for the synchronisation of the receivers is the GPS time scale. This architecture is different from the GSM and UMTS standards: networks using GSM or W-CDMA, the most common air interface of UMTS, are unsynchronised networks.

The time synchronisation requirements are specified by 3GPP2 (1999, C.S.0010), although the tolerance value is not written explicitly in this document. The document refers to the specifications of IS-95, which are not available in the public domain. However, publicly-available information suggests that all base stations must be synchronised within $\pm 2 \mu\text{s}$ of the GPS system time. In practice, this is achieved by using GPS-controlled oscillators at the base stations. The synchronisation requirements can be challenging to meet and they increase the operating costs of a CDMA2000 networks. The networks also need to keep operating without a GPS signal and the standard specifies that the synchronisation must be maintained within $\pm 10 \mu\text{s}$ of the GPS system time for eight hours after the GPS signal becomes unavailable. I noticed that most base stations had two GPS antennas, which may provide for redundancy of the time source but also indicates that a dependable and accurate time source is critical for the reliable operation of the network. Some major network providers in North America have started to switch their CDMA2000 networks to UMTS with W-CDMA since 2012. The Long-Term Evolution standard (3GPP - LTE) has been retained for the fourth-generation networks in North America, and this standard is an evolution of UMTS.

Existing work

I previously discussed GNSS aiding in unsynchronised networks. Synchronised networks have received more attention because their synchronisation and stability can be exploited to determine the user's position. The "Enhanced-911" mandate of the FCC, discussed in Section 1.3, has fostered research in this area because the FCC requirements could not easily be met using other solutions, for example using received signal strength. Caffery *et al.* (1998a) present a comprehensive overview of positioning methods in CDMA networks. They consider angle-of-arrival methods, which are generally suitable only at the base stations, and time-of-arrival methods. They also review the statistical properties of some time-of-arrival estimators.

I was not able to find relevant literature about the experimental analysis of the time stabilities of CDMA2000 signals. It seems that most positioning methods based on CDMA2000 signals assume perfect synchronisations and stabilities of the clocks generating the signals. Little information is available from the industry about the timing and synchronisation of CDMA2000 equipment.

All publications highlight the problem of position errors introduced by non-line-of-sight (NLOS) signals and provide different mitigation solutions. Later in this chapter, I will address the NLOS problem both at the TOA estimation and at the positioning levels. The assumption is generally made in the existing literature that the user position is tracked for at least several seconds or longer. Tracking improves the position accuracy because it exploits the accumulation of measurements, but it may also leave the users frustrated by the time required to determine their positions accurately. Algorithms that are designed to provide an almost instantaneous position are generally called "snapshot", or "push-to-fix". I only look at snapshot algorithms in this chapter.

Outline of the chapter

The work presented in this chapter is based on experiments on the synchronisation and stability of a CDMA2000 network. I first investigated the time stability of a CDMA2000 network with an outdoor antenna. The synchronisation of the signals with the GPS time scale allowed me to measure the propagation time of the signals. I analyse the statistics of the propagation time in both an indoor and outdoor environments in this chapter. I then consider a radio-positioning system based on the cellular signals. I present its performance here and illustrate some algorithms to improve the robustness and the availability of the position estimates. Finally, I exploit the synchronisation of the cellular signals with GPS to develop a positioning system that combines the signals

from both the GPS and the CDMA2000 network. I evaluated the performance of this system on indoor measurements, using a high-sensitivity GPS acquisition method, and I discuss the benefits of this approach at the end this chapter.

Acknowledgements

I carried out the experiments described in this chapter at the University of Calgary, Canada, in the “Position, Location, And Navigation” group. I received assistance from Professor Gérard Lachapelle, Dr Ali Broumandan, and Dr James T. Curran, who provided the experimental apparatus and the database of the BTS positions and identifiers.

5.2 Measurements of times of arrival of CDMA2000 signals

I carried out several experiments on the CDMA2000 network in different environments and propagation conditions. The apparatus common to all these experiments is presented in this section. Variations made to this baseline arrangement will be explained when appropriate in the remaining sections.

Structure of CDMA2000 signals

CDMA2000 is a code-division multiple access system in which all the transceivers of a network generally share the same frequency band. CDMA is provided by a direct-sequence spread spectrum modulation of the signal. Each logical channel is modulated by a different orthogonal spreading code so that all the logical channels can be transmitted on the same physical channel. The radio-frequency carrier is generally in a band around 800 MHz or 1900 MHz. The signal is spread twice on the forward link. The logical channels are first spread by a pseudo-noise sequence based on a Walsh code. Additional encoding, such as interleaving, convolutional error coding, etc. is then applied to most of the logical channels. Finally, the baseband signal is spread by a pilot PN sequence, whose generating polynomial is specified in 3GPP2 (2004a, §3.1.3.1.18). The signal goes through a baseband filter whose impulse response is specified in 3GPP2 (2004a, Table 2.1.3.1.18.1-1), which limits the bandwidth to about 1.23 MHz.

The Forward Pilot Channel is transmitted by every base station in order to synchronise the mobile receivers. The Forward Pilot Channel is assigned the Walsh function 0 and does not undergo any further processing: it is a direct modulation of the RF carrier by the pilot PN sequence. The pilot PN sequence is a quadrature sequence composed of

2^{15} chips transmitted at a chip rate of 1.2288 Mc/s, resulting in a repetition period of $T_{\text{pilot}} = 80/3 = 26.6\bar{6} \dots$ ms.

The base stations are identified by the offset index of the pilot PN sequence. The origin of the pilot PN sequence is delayed by $64N$ chips, where N is the *offset index* that identifies the base station. The granularity of 64 chips implies there is a maximum of 512 base stations visible from any point of the network. The transmission range of a base station must also be limited so that the code-phase delay introduced by the propagation time of the signal remains within the same PN offset index. The length of 64 chips thus limits the maximum range to about 15.6 km. This limit must be enforced by the network operator, even if the transmitting power of the BTS equipment is allowed a greater range, otherwise interference between base stations may be introduced.

Some CDMA2000 channels may use faster spreading rates and wider bandwidths. In particular, spreading rates of three times and five times are available on many channels. I did not investigate these channels, as they are not explicitly designed to provide time synchronisation and their availability is uncertain. However, their wider bandwidths may be of interest for future work.

Previous work on time estimation in multipath channels

The bandwidth of the CDMA2000 synchronisation signal is not wide enough to characterise the full impulse response of the channel, i.e. all the propagation paths can not be resolved. Thus, it is not possible to resolve the arrival times of all of the signals coming from different paths and the possibilities of multipath mitigation are limited. Faragher (2007) showed that, by the effects of convolution of the channel impulse response in a narrow bandwidth, the earliest correlation peak may actually occur before the signal has arrived.

Most of the existing work on multipath mitigation does not apply directly to our problem. Existing publications generally assume that filtering the measurement stream over time is possible, whereas we are interested in “snapshot” positioning, where the position is calculated with typically less than 500 ms worth of measurements. Fleury *et al.* (1999) proposed to use the space-alternating generalized expectation-maximisation (SAGE) algorithm to estimate the channel parameters. The parameters were the signal amplitudes, the path delays and the directions of arrival of the signals. The direction of arrival could be determined because they used an antenna array. The SAGE algorithm was introduced by Fessler *et al.* (1994) as a method to find the maximum-likelihood parameters of a probabilistic model. It is a variant of the expectation-maximisation (EM) algorithm developed by Dempster *et al.* (1977), an iterative method to estimate

the maximum-likelihood parameters of a likelihood function. The SAGE approach improves the convergence speed for a class of problems and has been widely used for the estimation of communication channels. The SAGE algorithm applied to TOA estimation is similar to super-resolution methods, such as the multiple signal identification and classification (MUSIC) algorithm and the estimation of signal parameters by rotational invariance techniques (ESPRIT) algorithm. For example, MUSIC was used by Klukas (1997) to improve the TOA estimation of signals on the Advanced Mobile Phone System. Leon *et al.* (2006) and Li *et al.* (2009) compared the performance of MUSIC, ESPRIT, and SAGE, and concluded that the SAGE algorithm gave the smallest mean squared error.

The SAGE algorithm can be used to reduce the effects of multipath propagation, however this method has some limits. First, SAGE can be computationally demanding and it is sensitive to the actual number of multipath components, which is generally unknown and assumed to be fixed. Another problem is that the largest peak is not necessarily the first arrival, since multipath can attenuate the line-of-sight component below the strengths of the non-line-of-sight components at time. In this condition, the LOS signal may fall below the detection threshold and the estimator will not find the LOS signal. Finally, the SAGE estimator is still limited by the channel bandwidth, which is not wide enough to allow for a fine resolution of the channel impulse response.

Signal model in presence of multipath propagation

The received signal at baseband is represented by $z(t)$. We assume the channel has an additive white Gaussian noise of dual-sided power spectral density N_0 . It is a multipath channel composed of N_p paths, with a flat-fading profile and is not frequency selective. We note $g(t)$ the replica of the transmitted signal, $g(t) = c_p(t) * h(t)$, where $c_p(k)$ is the pilot PN sequence and $h(t)$ is the impulse response of the pulse-shaping filter. The received signal, after baseband downconversion and sampling, is modelled by

$$z(t_k) = \sum_l^{N_p} a_l g(t_k - \tau_l) e^{j2\pi \delta f t_k} + \sigma v(t_k) \quad (5.1)$$

where t_k is the sampling instant, a_l is the complex amplitude of the l -th path, τ_l is the code phase of the signal from the l -th path, and δf is the residual frequency offset after downconversion. We seek to estimate τ_l from the received samples. We define two vectors of parameters, the vector of amplitudes, $\mathbf{a} = [a_0, \dots, a_{N_p}]$ and of code phases, $\boldsymbol{\tau} = [\tau_0, \dots, \tau_{N_p}]$. $v(t_k)$ is a sequence of normal complex random variables such as $\langle v(t)v^*(t') \rangle = 2\delta(t - t')$. The synchronisation parameters are the PN code phase and the frequency offset.

The three estimators of the code phase parameter are discussed in the rest of this section. The time-of-arrival estimate of the signal is calculated from the code-phase estimate by removing the constant offset index used to identify the BTS. The signal is detected using a generalised likelihood-ratio test (GLRT), as presented in Chapter 2, with a coherent integration period of $3T_{\text{pilot}} = 80$ ms. This choice represents a compromise between longer integration times to improve the detection probability and shorter integration times to reduce the sensitivity to frequency offset mismatch. Besides, an integration time that is an integer number of periods of the GPS C/A code facilitates the synchronisation of the measurements with GPS time. The recommended maximum Doppler shift to limit the losses during the coherent integration is 6.25 Hz, corresponding to a maximum velocity of 3.5 km/h at the RF frequency of the CDMA2000 network. I was careful to walk slowly enough while making the experiments.

The stabilities of the oscillators at the receiver and the BTSs were such that I did not have to adjust the frequency offset even for measurements made three weeks apart. All the base stations of a same network provider transmitted on the same frequency, thus the frequencies offsets of all the signals received by a static receiver were the same. Both the receiver and the transmitting BTSs were static hence the frequency offset δf was determined once for all the base stations and for the duration of the experiment. The frequency offset was removed from the search space, which then consisted only of the possible PN pilot code phases.

Three methods to estimate the times of arrival

I used three different estimators of the times of arrival for the calculations presented in the rest of this chapter:

- the single-path, maximum-likelihood estimate, which is the same as the code-phase estimation method based on the generalised likelihood-ratio test presented in Chapter 2, and is the maximum-likelihood estimator under the single-path assumption, i.e. it is optimal only if $N_p = 1$;
- a heuristic estimator, which is similar to the code-phase estimator except that it gives more than one estimate, in an attempt to estimate the multipath components. The estimated parameters is the set, $\hat{\Theta}$, of all the code phases that give a local maximum of the likelihood ratio above the detection threshold, η . This set is more formally defined as

$$\hat{\Theta} = \left\{ \forall \tau \in [0, T_{\text{pilot}}) \mid \Lambda(\tau) > \Lambda(\tau - T_s) \text{ and } \Lambda(\tau) > \Lambda(\tau + T_s) \text{ and } \Lambda(\tau) > \eta \right\},$$

where $\Lambda(\tau)$ is the likelihood ratio of the signal, defined in Equation 2.12; and

- a SAGE-based estimator, which employs the SAGE estimator to calculate the maximum-likelihood values of the amplitudes and delays parameters. The likelihood function of the signal for the amplitude and code-phase parameters is

$$\log \mathcal{L}(\mathbf{a}, \boldsymbol{\tau} | \mathbf{z}_{1:N}) \propto E_z - 2 \operatorname{Re} \left[\sum_{k=1}^N z_k \sum_{i=0}^{N_p} a_i^* g^*(t_k - \tau_i) \right],$$

where N is the coherent integration length, and $\mathbf{z}_{1:N}$ is a vector of N samples of the received signal. The parameters estimated by SAGE are thus

$$(\hat{\mathbf{a}}, \hat{\boldsymbol{\tau}}) = \arg \max_{(\mathbf{a}, \boldsymbol{\tau})} \mathcal{L}(\mathbf{a}, \boldsymbol{\tau} | \mathbf{z}_{1:N}).$$

A decision rule keeps the earliest code-phase estimate in the delay vector whose associated amplitude crosses the detection threshold η .

Choosing the number of paths is a well-known problem when modelling a propagation channel. Different techniques have been investigated, for example Wax *et al.* (1985) used the minimum description length as an information criterion. Most of these methods are computationally expensive since they iterate the SAGE algorithm over different values of N_p . My implementation of the SAGE algorithm did not estimate the number of paths. I calculated the value of the maximum likelihood for different number of paths for the signals coming from BTS 440 and over a sample of outdoor measurements. The maximum likelihood was obtained for three paths and I kept this value for the rest of the analysis.

SAGE is an iterative algorithm and I used a stopping rule based on a fixed threshold on the residual delay and amplitude steps. I found that few iterations were required. For many base stations, the estimates were almost unchanged after the first iteration. In these situations, the algorithm is similar to the successive-interference-cancellation (SIC) scheme, as described by Patel *et al.* (1994). In many situations, the SIC scheme may provide results similar to SAGE while being less computationally demanding.

Experimental details

I collected the data in the laboratory of the “Position, Location, And Navigation” group at the University of Calgary, Canada. The experimental arrangement was built around a National Instrument (NI) radio-frequency vector signal analyser with three channels. Each channel consisted of a NI PXI-5600 RF receiver, followed by a NI PXI-5142 signal digitizer. The samples were streamed directly onto an array of 15 hard-disk drives, thus enabling the high data transfer rates required to record the

signals continuously acquired by the three channels. I configured the instrument for a 10 MHz input bandwidth and a 10 MHz baseband sampling rate. The recorded data were the in-phase and quadrature samples of the baseband signal.

Different sets of antennas were used. For outdoor measurements, I used the GPS and CDMA2000 antennas permanently installed on the roof of the “Centre for Communications and Information Technologies” building. For indoor measurements, I used a patch antenna for GPS and a quarter-wavelength dipole for CDMA2000 signals. The CDMA2000 antenna was followed by a ZHL-1217 low-noise amplifier with a gain of about 30 dB and noise figure of 1.5 dB, and an RF pre-amplifier of gain 20 dB and noise figure 5 dB. Low-noise amplifiers with gains of about 23 dB were integrated to the GPS antennas. A pre-amplifier with a gain of 20 dB was also added to the GPS antenna for indoor experiments. The three acquisition channels were synchronised together with common clock and trigger signals. One of NI PXI-5600 RF receivers provided the clock signal from an OCXO with an accuracy of 50 ppb and a stability of 20 ppb/year. The lengths of the cables to the roof-top antennas were unknown and I assumed there was no significant length difference between the signal paths of the GPS and the CDMA2000 channels.

All the measurements I made are divided into two series in this chapter. The outdoor signals were recorded as sequences of duration 30 seconds each, repeated every 24 minutes for 90 hours. The interval between acquisitions was longer than the one used for the GSM experiments presented in Chapter 4 because the sampling rate of the NI frontend was higher, thus filling the available storage space more quickly. I did not reduce the sampling rate or decimate the signal in order to exploit the widest bandwidth possible to study the channel propagation characteristics. I recorded this data set during the Thanksgiving week-end in November 2011. There was little activity in the buildings surrounding the receiver. This area of the city was composed mostly of two-story houses, with taller buildings on the university campus and a nearby hospital. The building was located in a valley surrounded with low-height hills. I would subjectively classify the outdoor propagation characteristics as those of a moderate urban environment.

The set of indoor measurements was smaller, consisting of eight sequences lasting 37.5 seconds each. The first six sequences were collected on the 21st November 2011 and the last two sequences on the 29th November 2011. Each sequence corresponded to a different location of the indoor antenna in the laboratory room. In some sequences, the antenna was moved to represent the motion of a pedestrian. I will make reference to the configuration of a specific sequence when necessary. One of the acquisition channels

was always connected to the GPS outdoor signal for all experiments. I extracted the GPS time from this signal and used it to compensate for the drift of the signal analyser's oscillator.

I did not observe any near-far effect, which often degrades CDMA signals. The near-far effect is caused by the difference in signal strength between the nearest and furthest transmitters: the dynamic range of the receiver may not be large enough to detect the weakest signal. This effect is specific to CDMA communications, where all the signals continuously occupy the same spectral band. The NI PXI-5600 frontend had a spurious-free dynamic range of 80 dB and the NI PXI-5142 had a 14-bit ADC, or about 84 dB of dynamic range. The dynamic range of the receiver was thus about 80 dB, which accommodated the difference of signal strength between the strongest signal, from BTS 232, and the weakest one, from BTS 292. The near-far effect is problematic in mass-market receivers, whose dynamic ranges are smaller than the apparatus used for the experiments. The CDMA2000 standard helps mitigate the near-far effect by continuously adapting the power of the signals transmitted by the mobile stations, so that the noise floor is not significantly increased in the area around the transmitter. Another solution is the virtual cumulative blanking method proposed by Duffett-Smith *et al.* (2002).

5.3 Time stability and synchronisation of CDMA2000 networks

The CDMA2000 standard specifies that the pilot signal must be synchronised within $\pm 2 \mu\text{s}$ of the GPS time, but the stability of the synchronisation is not specified. An oscillator of the type seen in Chapter 4, for example, may present quasi-periodic instabilities within $\pm 2 \mu\text{s}$ and still satisfy the synchronisation requirement. There does not seem to be any publicly-available information about the synchronisation characteristics of real networks. Therefore I measured the time stabilities of the pilot signals of seven CDMA2000 base stations.

Signal strength

The experimental arrangement was similar to the one described in Section 5.2, using outdoor antennas. The time-of-arrival errors were calculated using the distances between the BTS positions in the database and the surveyed position of the CDMA2000 antenna at the receiver.

The post-detection signal-to-noise power ratio is shown in Table 5.1. The SNR is estimated from a simple mean-variance estimator, which may be biased and not statistically robust. However, the results give an idea of the range of signal strengths. There was no significant multipath fading in the outdoor signals. The receiver and the transmitter were all static, although the presence of several roads with dense traffic could have provided some dynamic scatterers near the receiver.

Table 5.1: Post-integration signal-to-noise ratio.

BTS	SNR (dB)
80	19.8
164	15.0
180	9.4
232	39.8
292	6.1
356	10.0
440	29.1

Time synchronisation

I calculated the time differences between the theoretical and observed times of arrival of the pilot signals. The theoretical time of arrival was calculated from the GPS time, the PN offset of the base station, and the distance between the receiver and the BTS. The observed times of arrival were estimated by the SAGE algorithm.

Table 5.2: Pilot signal TOA error, theoretical - measured.

BTS	Median error (μ s)	Standard deviation (μ s)
80	-0.33	0.13
164	0.08	0.05
180	0.27	0.12
232	1.98	0.04
292	-1.63	0.15
356	-16.47	0.20
440	1.66	0.05

The statistics of the universal time errors of the pilot signals are presented in Table 5.2. All of them are within the synchronisation requirement of 2μ s, except for BTS 356.

BTS 356 was located on one of the tallest building in the city centre and thus had longer range than most base stations. It is possible that this BTS had a visible range

larger than the 15 km required to maintain the maximum code delay within a same offset index of the BTS. A delay of 16 μ s, about 5 km, may have been introduced to apparently move the BTS away from its interference zone. This possibility is reinforced by the fact that the PN offset index of this BTS was never reused in the entire city, contrary to most of the other BTSs. Another possibility is that there was an error in the BTS database, although this would imply that the base station was even further than it appeared, which is unlikely. BTS 232 was close to the 2 μ s limit, although there was a wider margin when I did not use the SAGE algorithm.

The time synchronisation errors can not be explained away by a difference in the path lengths of the GPS and CDMA2000 signals at the transmitters, introduced for example by different cable lengths. I noticed that the GPS antennas of most BTSs were situated close to the equipment room, at the bottom of the mast supporting the CDMA2000 antennas at its top. But the errors observed are one order of magnitude larger the errors that could be introduced by the mast heights, which look at most 30 m high. We will consider, in the rest of this chapter, that the values presented in Table 5.2 are the constant biases of the BTS clocks and we will use these values to correct the TOAs when needed.

Time stability

We have studied the average time synchronisation of the network and we now focus of the time stability of the signals. The time stability was analysed using the single-path estimator. I did not apply a detection threshold for these measurements as the goal was to utilise as many data points as possible. This introduced some outliers for the BTSs with the weakest signals, since the maximum correlation peak may have been caused by the noise alone. I applied a Kalman smoother to remove these outliers and I excluded BTS 292, which had the weakest signal, from this rest of the experiments in this section.

The Kalman smoother used a simple random-walk model and an innovation gate that rejected measurements outside a 3σ normalised innovation squared. The measurement noise is a combination of the uncertainty in the TOA estimation and the uncertainty in the GPS time estimation. The sample standard deviation of the TOA measurements is shown in Table 5.2 and I assumed that it was representative of the measurement noise, i.e. that the network was perfectly stable. I chose 0.5 μ s as a conservative value for the standard deviation of the measurement noise. The standard deviation of the Gaussian random walk was arbitrarily set to 1 ns/s, a value typical of OCXO oscillators. I gave the process noise a rather large variance intentionally, since

the smoother was simply used to remove the outliers. The goal was to give the most flexibility to the process model.

The smoothed time series of the TOA errors are presented in Figure 5.1. The stability of the pilot signal was excellent. It looked as if the BTS oscillators were always locked on the GPS time and had excellent long-term stabilities. I observed some short-term fluctuations, some of which periodic and with a period close to 24 h. These may have been caused by daily changes in the temperature. The local time and the drift of the local clock were estimated at every acquisition using the GPS data, so the changes in temperature of the receiver should not have affected the results. The amplitudes of these variations were smaller than 200 ns for all the base stations.

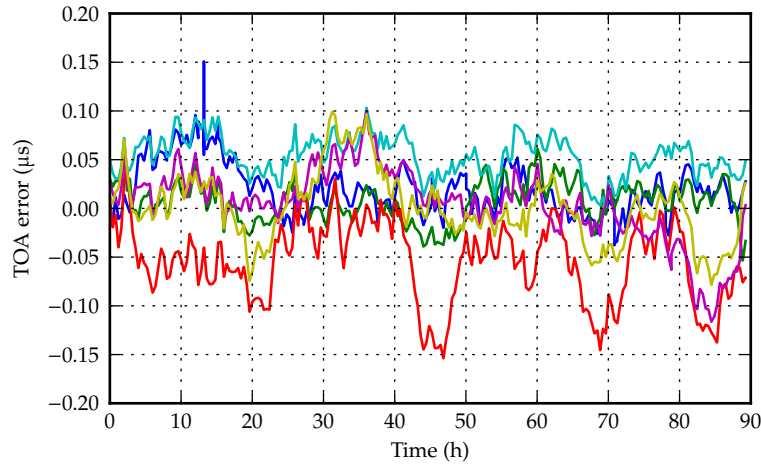


Figure 5.1: Time series of the TOA errors, smoothed by a Kalman filter using a random walk process model. The TOA has been offset to have a null error at the time origin. BTS 292 is excluded as it generally falls below the detection threshold.

The cause of the remaining time deviations is difficult to establish. The GPS software receiver I designed employed a delay-locked loop with a spacing of 100 ns and a tracking bandwidth of 20 Hz. The C/N_0 of the signal was large, generally about 48 dB-Hz, hence the noise introduced by the GPS time estimation was negligible. (For a more complete treatment of performance bounds in tracking loops, one can refer to Parkinson *et al.* (1996, chapter 7)). The two most likely sources of fluctuations are thus the stochastic nature of the BTS oscillators and the TOA estimation errors, in particular caused by propagation in an urban environment.

Conclusions

The times of arrival the CDMA2000 pilot signals of the seven base stations studied are within $2\text{ }\mu\text{s}$ of GPS time, except for one base station, and the time stability is better than 200 ns over a period of 90 hours. This suggests the CDMA2000 transmitters have stabilities similar to those of the GPS master clock and are continuously synchronised with the GPS time, with a constant clock bias error. The BTSs probably used disciplined oscillators continuously locked onto the GPS signals.

5.4 Error analysis of the propagation time

We now make the assumption that the CDMA2000 pilot signals are perfectly synchronised with GPS time, up to a constant clock bias. This assumption may not be entirely correct as we noted some periodic variations which may indicate that the signals are affected by temperature changes. However, it enables us to calculate the propagation times of the signals with only one receiver. Experiments to study the propagation times, such as those carried out by Faragher *et al.* (2010), generally require two synchronised receivers. One receiver is located close the transmitter, at a place where the signal propagation is little affected by the environment. The second receiver, synchronised with the first, makes the measurements at the locations of interest. By using a CDMA2000 receiver synchronised with GPS time we can calculate the propagation times with only one receiver, since the CDMA2000 transmitters are also synchronised with GPS time.

In this section, I present an analysis of the estimation errors of two time-of-arrival estimators, both in an indoor and outdoor environments.

Sources of errors

TOA measurements are affected by different types of uncertainties. Some of these uncertainties are noise processes that can be estimated reasonably well. These include, for example, the phase noise and the sampling noise. Others, such as the ones caused by the uncertainties and randomness of the propagation channel, are more difficult to analyse.

The oscillators in the signal analyser and at the base stations introduce some errors in the TOA measurements. The long-term drift of the local oscillator is compensated using the GPS measurements and I assume that the short-term fluctuations of the TCXO in the RF frontend are negligible. The time deviations of the BTS oscillators are not directly observable. I will assume that they are negligible, although we noted

quasi-periodic time variations for one of the base station. The sampling period is 10 ns and the analog-digital converter has more than 80 dB of dynamic range, hence the quantisation noise can also be neglected.

The statistics of the TOA estimation error have been calculated for an additive white Gaussian noise channel, without multipath, in Section 2.1. The estimation errors in a multipath channel are more difficult to estimate and are part of an active research area. Many analytical models of propagation channels have been proposed and most of them are derived from physical considerations backed by empirical measurements. They sometimes only address the calculation of the signal strength or the signal fading properties in a multipath environment, and the statistics of the individual paths are not available. The Nakagami model (Nakagami, 1960) is commonly used to represent a fading environment and several models have been proposed to predict the average signal strength and the capacity of mobile communication systems. These do not attempt to model the propagation times.

We are more interested in the timing models of multipath propagation. Many models of multipath propagation depend on parameters that are specific to a particular environment, such as the number of paths, the position of the reflectors and scatterers, etc. Saleh *et al.* (1987) developed one of the most commonly used models in indoor environments, generally known as the Saleh-Valenzuela model. They present the power profiles of measurements in an indoor channel and note that the signal arrivals form clusters. They develop an analytical model where the arrival of a cluster and of the signals within a cluster are both modelled as Poisson processes. The arrival times thus follow an exponential distribution. The Saleh-Valenzuela model, as most analytical models, is generally used for simulation and evaluation purposes, and not directly for improving the propagation time estimation. We will consider this model for the indoor measurements of propagation times of CDMA2000 signals.

Experimental details

The experimental arrangement was similar to the one described in Section 5.2. I considered two types of estimators: the SAGE and the single-path maximum-likelihood estimators. The TOA errors were calculated by removing the offset indices of the BTSs, the constant time biases shown in Table 5.2, and the theoretical propagation times.

The previous section did not address the detection problem; all the measurements were used by the Kalman smoother, and a gating process based on the likelihood ratio of each sample was used to reject outliers. I added a likelihood-ratio test for the remaining experiments of this chapter. I chose a detection threshold of $\eta = 4$, which

gave a probability of false alarm of about 0.13, using Equation 2.15. I did not perform any additional non-coherent integration. The same threshold was applied to each of the three estimators.

Analysis of outdoor signals

The distribution of the TOA errors, estimated using SAGE, is shown in Figure 5.2. The shapes of the histograms of the TOA noise of BTS 232 and BTS 440, in Figures 5.2(d) and 5.2(f), suggest the time distribution has thicker tails towards late arrival times. The probability plots of BTS 80, BTS 180, and BTS 356, show that the early arrival times are more frequent than those predicted by a Gaussian arrival time distribution, e.g. longer tails for early arrivals.

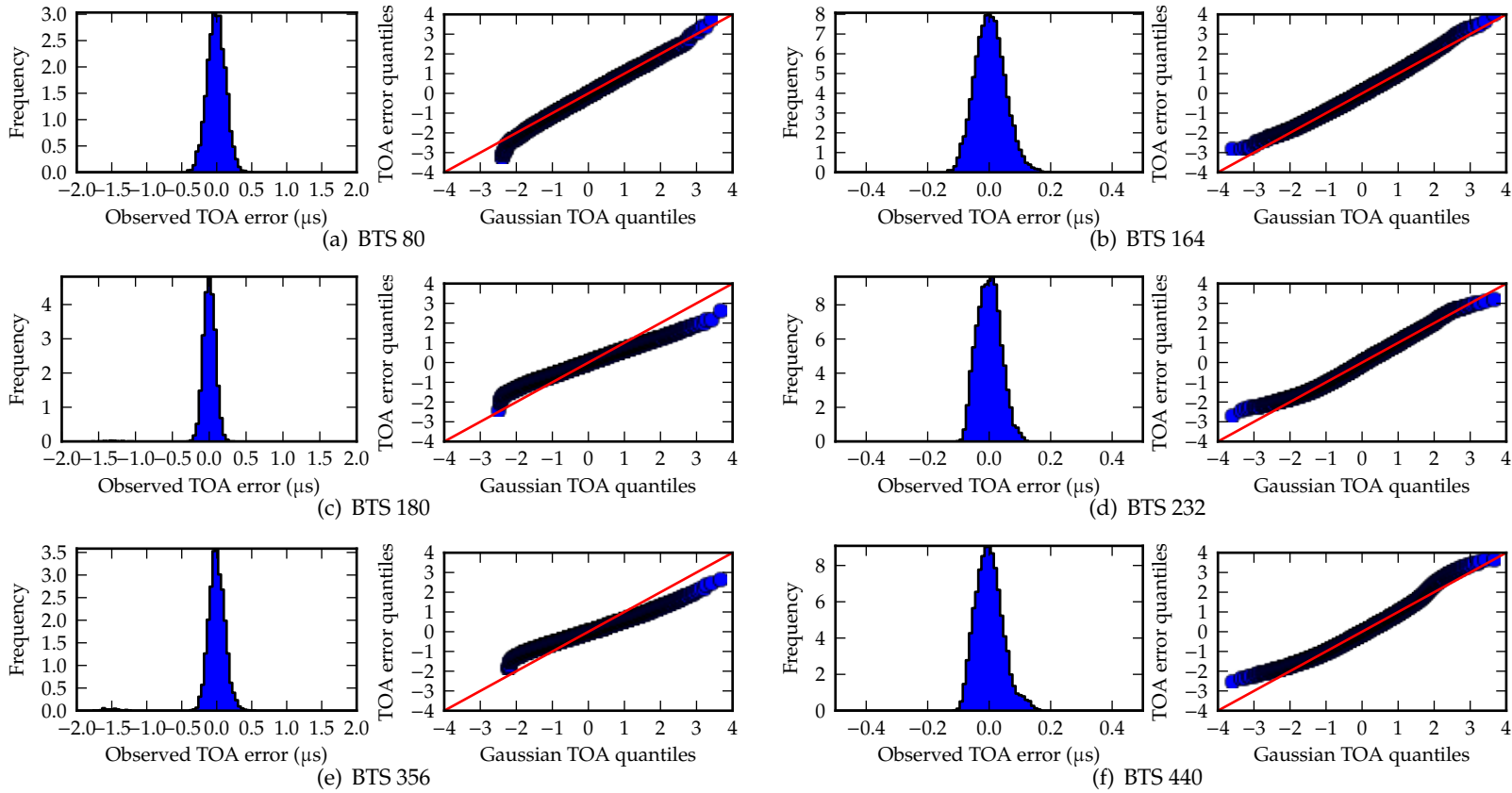


Figure 5.2: Time-of-arrival errors, using SAGE-based peak detector.

We first calculate the CRLB of the TOA estimator, using Equation 2.8. I calculated the effective channel bandwidth of the CDMA2000 Forward Pilot Channel to about $\beta = 1.1$ MHz, based on the pulse-shaping filter response. The theoretical standard deviation and the observed standard deviation, which are recalled from Table 5.2, are presented in Table 5.3. The values are generally four times larger than the minimum standard deviation of the estimator, with significantly worse standard deviation for BTS 80, BTS 232, and BTS 440. The difference may be attributed to the propagation channel or the stability of the oscillators, as mentioned in Section 5.4.

Table 5.3: Comparison of the Cramér-Rao bound of the TOA estimator and the observed standard deviation.

BTS	SNR (dB)	Lower bound (ns)	Observed deviation (ns)
BTS 80	19.8 dB	11	135
BTS 164	15.0 dB	18	49
BTS 180	9.4 dB	35	78
BTS 232	39.8 dB	1	38
BTS 356	10.0 dB	32	112
BTS 440	29.1 dB	4	44

The TOA errors of the outdoor signals fit a Gaussian distribution reasonably well in the range of $\pm 2\sigma$, where σ is the sample standard deviation. The distribution of the estimated TOA errors is however more skewed towards early arrival times for the BTS 80, BTS 180, and BTS 356; negative errors of magnitude larger than two standard deviations are more exceptional than for the Gaussian fit. This is probably a consequence of the SAGE estimation algorithm, which privileges early arrival times. This anomaly is not observed on the other BTSs, where, on the contrary, early arrival times have stronger probabilities than the Gaussian fit. This too may be explained by the behaviour of the SAGE algorithm: we perform the TOA estimation in a multipath environment under the assumption of a constant number of paths for all base stations. BTS 232 and BTS 440 have the strongest signals and the presence of secondary paths is clearly visible in the histograms of the TOA. The SAGE algorithm thus correctly estimates the parameters of these secondary paths, which gives less freedom to identify earlier arrival times. The secondary paths were not visible in the measurements from the other BTSs, thus giving more opportunities for the algorithm to identify early paths. We do not observe a significant skew towards later arrival times, as would be the case in a multipath environment where the arrival times of the secondary paths follow a Poisson process.

Analysis of indoor signals

The distributions of the TOA errors of the pilot signals in an indoor environment are shown in Figure 5.3, using the SAGE algorithm, and in Figure 5.4 using the single-path maximum-likelihood estimator.

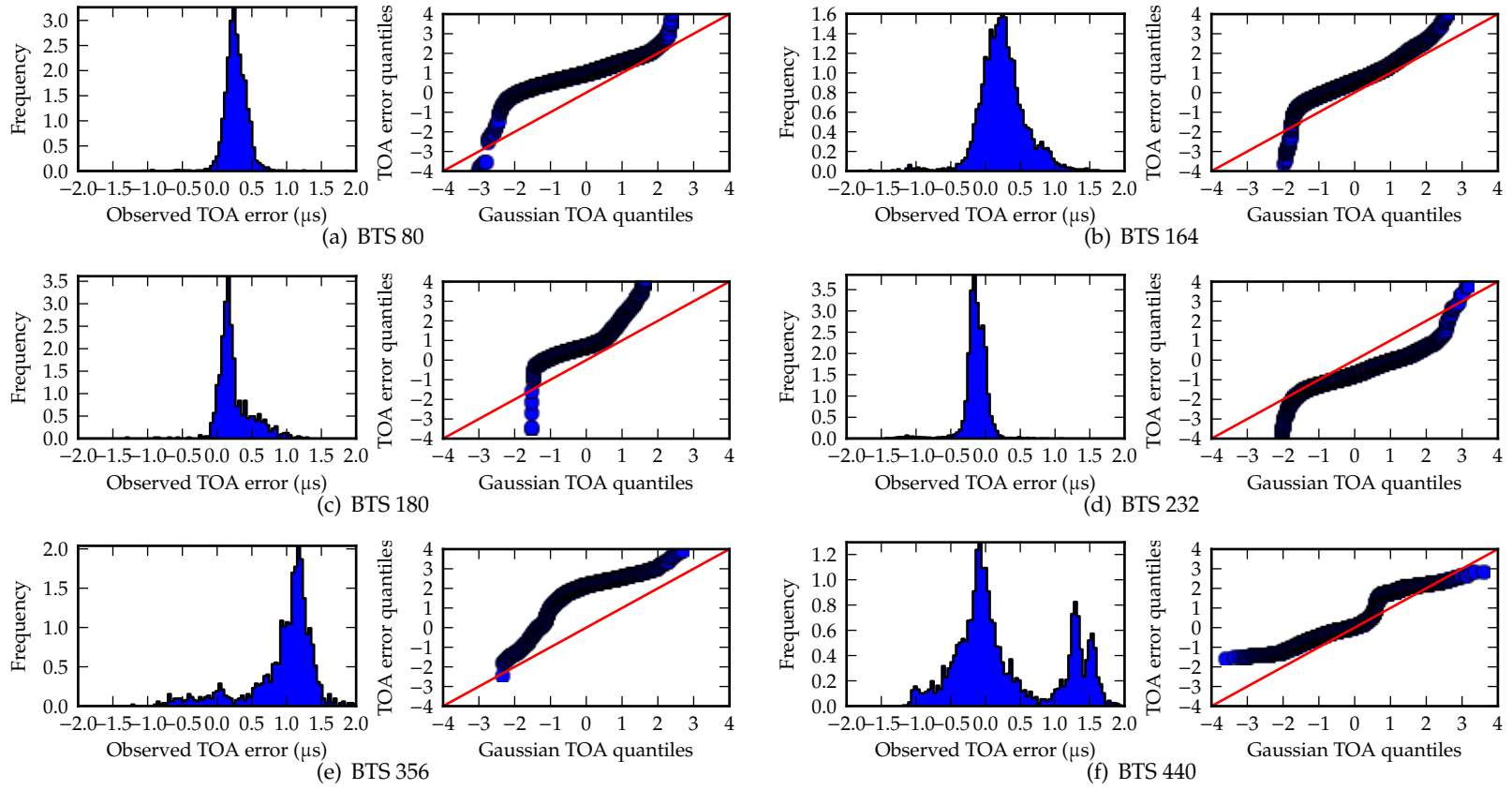


Figure 5.3: Time-of-arrival errors, using SAGE-based peak detector.

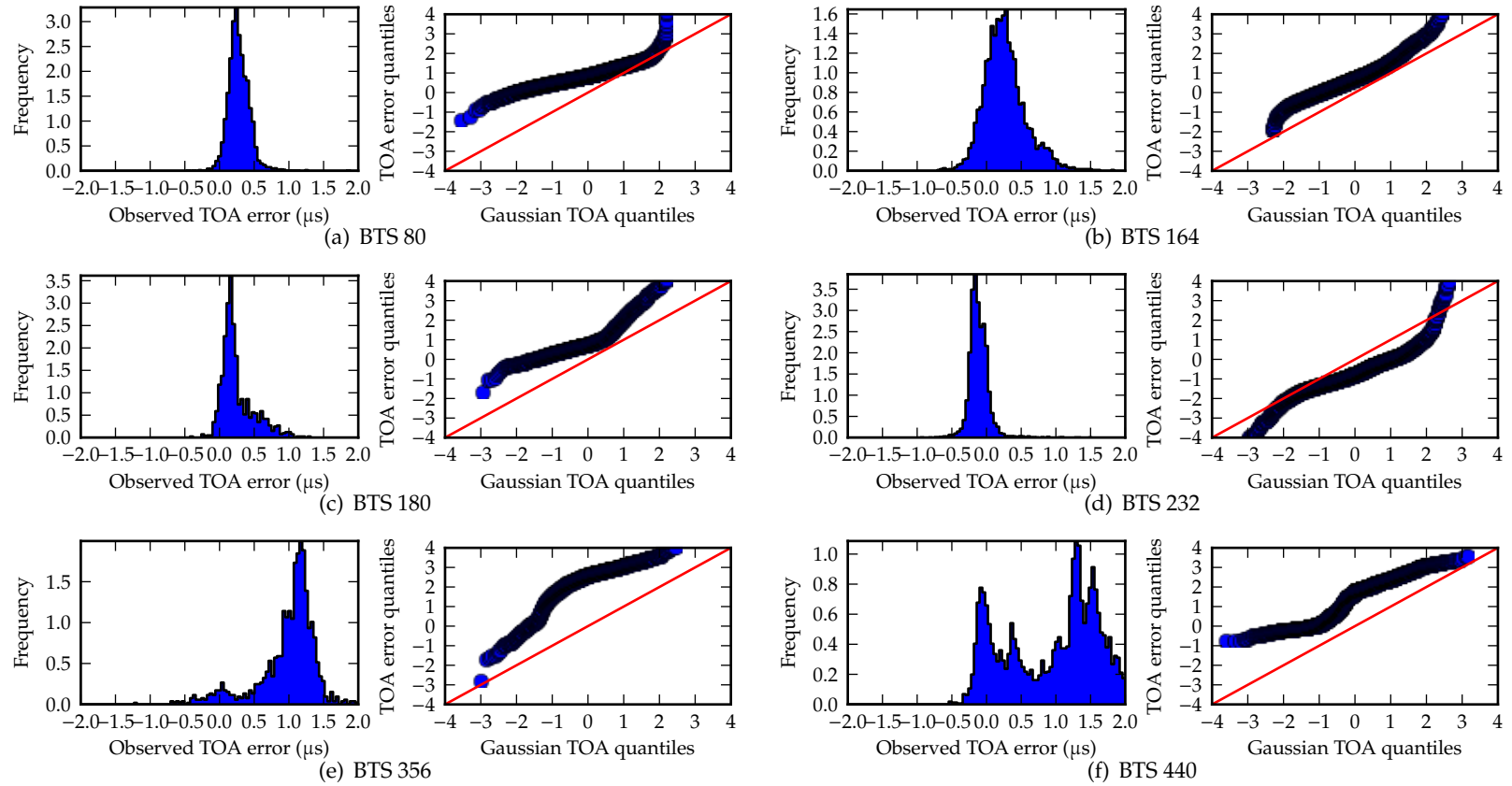


Figure 5.4: Time-of-arrival errors, using correlation peak maximum.

Unsurprisingly, the error distributions of the times of arrival of indoor signals are more complex than in the case of outdoor signals. There is no major difference between the performance of the SAGE algorithm, shown in Figure 5.3, and the single-path ML algorithms, shown in Figure 5.4. The Gaussian fit is generally poor, except for BTS 80 and BTS 164. I did not calculate the standard deviation because such descriptive statistics would not be meaningful without a better characterisation of the error distribution. The TOA error distributions are generally biased towards late arrival times, which indicates that even the SAGE algorithm is not capable of identifying reliably the shortest path components in these signals. However, the SAGE algorithm does reduce the occurrence of some early TOA errors. The worst estimation errors occur with signals from BTS 356 and BTS 440.

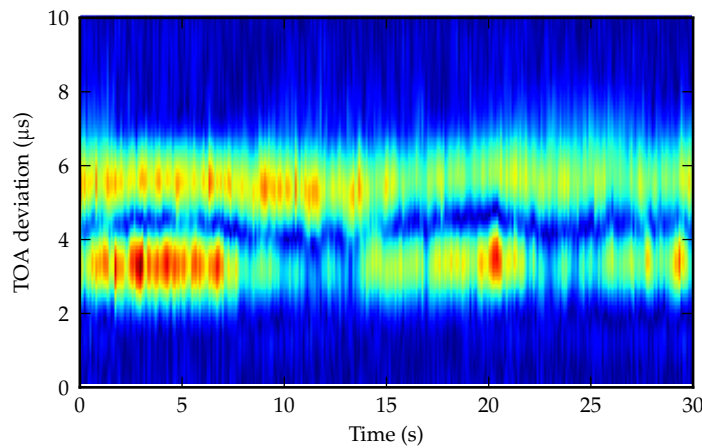


Figure 5.5: Illustration of multipath fading, power profile of BTS 440.

The SAGE algorithm has a limited effect on the TOA estimation of BTS 440 because the signals from that BTS can propagate along two paths with almost equal probabilities. The strengths of these two components are almost similar, hence the histogram of the single-path estimator (Figure 5.4(f)) has two modes of approximatively equal frequencies. Figure 5.5 shows the power profile of the fading caused by the multipath propagation of the channel. In this example, the receiver was static and the correlation time of the multipath fading was several integration periods, generally between 400 ms and 1.2s. The signal fading of the two main paths is not an independent process, since a fade occurring on one path tends to corresponds to a stronger signal along this other path, thus keeping the total energy constant. The SAGE algorithm often fails to recover the earliest arrival time as the strength of the early ray is below the detection threshold. However, the magnitude of the secondary peak in the histogram

of Figure 5.3(f) is smaller than in Figure 5.4(f), thus highlighting the advantage of the SAGE-based estimator.

The case of BTS 356 is interesting, as it shows a systematic bias of $1.2\ \mu\text{s}$ which can not be corrected by any algorithm. This BTS is the tallest one and this may lead to a greater probability of being in sight of a reflector that may provide a strong non-line-of-sight signal to the receiver. It is possible that most of the techniques based on maximisation of the likelihood of a single signal fail in this situation, since the likelihood function is generally maximised by the strongest ray. A joint likelihood function, which includes the signals from all the base stations and a model of biases, may help in this situation. This scheme will be discussed later in this chapter.

5.5 Positioning using cellular signals only

We now exploit the synchronisation of the BTSs to determine the position of a mobile receiver. This method is similar to the Advanced Forward-Link Trilateration (AFLT), specified in the standard 3GPP2 (2004c, C.S0022-A). I have not been able to find any experimental evaluation of AFLT or any report about the usage of AFLT in real networks. I present the results of indoor and outdoor experiments.

Positioning in an urban environment or indoors is generally challenging because most of the signals propagate in multipath conditions and the TOA measurements are often made of non line-of-sight signals. The TOA estimators presented in the previous section cannot completely eliminate the effects of multipath propagation and NLOS conditions. For example, Figures 5.3(e) and 5.3(f) show that the times-of-arrival of the signals from BTS 440 and BTS 356, using the SAGE estimator, are incorrect because of non line-of-sight propagation. We review and evaluate two algorithms that help mitigate the effects of non line-of-sight propagation.

Positioning with NLOS signals

The analysis of the TOA error distribution, in Section 5.4, has highlighted the effects of multipath propagation. The indoor signals are all non line-of-sight and suffer from systematic delays, such as the signals from BTS 356, or delays varying between two discrete values, for instance the signals from BTS 440. Multipath propagation and non-line-of-sight measurements are generally found together. The term multipath is often associated to the problems of channel and TOA estimations, whereas NLOS is more commonly found when talking about position calculation.

The robustness of the positioning algorithm can be improved in order to cope with NLOS signals. Robust statistics is a research area that deals with improving the performance of an estimator when the input data break the assumptions made by the estimator. The TOA estimated from non-line-of-sight signals break the Gaussian and line-of-sight assumptions of the algorithm used for positioning. The effects are variable, from a systematic bias of a hundreds of meters, to the divergence of the iterative procedure and, in the worst case, the convergence to a grossly incorrect solution. We now review several robust positioning methods that have been proposed to mitigate NLOS conditions.

A first class of methods seeks to classify whether each measurement belongs to a LOS or NLOS signal, before any position is calculated. Fischer *et al.* (1998), presenting the results of simulations, address the detection of NLOS measurements by comparing the sample variances of the pseudo-range measurements. Measurements whose variances are larger than the average variance are treated as NLOS. Wylie-Green *et al.* (2001) consider a channel with intermittent NLOS conditions. A set of measurements is collected for every transmitted signal and they calculate the probabilities of LOS or NLOS for every measurement. These probabilities are propagated by a transition model, which depends on the speed of the mobile, and updated by the measurement likelihood. The calculations are performed over sub-sets during which the user is assumed to be in the same area, such that the user motion is masked by the measurement noise. The TOAs of the LOS measurements are described by Gaussian random variables with fixed means, while the TOAs of the NLOS measurements have an additional positive random variable. They propose an algorithm that propagates the probabilities of LOS and NLOS of each measurement and present the results of simulations.

A different approach consists in using the results of the position calculation to detect the NLOS components in the original measurements. Pi-Chun Chen (1999) proposes the calculation of the least-squares positions for all possible combinations of measurements, then take the average position weighted by the reciprocal of the residuals. This approach is computationally demanding as it requires to solve the position equation $\sum_{i=3}^N \binom{N}{i}$ times for a 2D-position, where N is the number of input signals. It improves the robustness of the iterative least-squares method but it does not specifically address NLOS signals, ignoring, for example, the property that NLOS signals are more likely to arrive later than the LOS signals.

The two categories of methods we have presented above try to address the problem at two different stages: some methods work on the measurements while others work on the results of the calculation. It is possible to combine these methods in order to

embed the probabilities of LOS and NLOS into the position calculation. Cong *et al.* (2004) investigate this approach and they compare two algorithms. The first algorithm successively rejects the combinations of measurements based on their residuals. The second algorithm takes a probabilistic approach, which relies on prior probabilities of LOS and NLOS of every measurement. The joint probability density function of the position is then calculated. The measurement likelihood function of the LOS path is a Gaussian model, and a combination of Gaussian model and exponential arrival time for the NLOS path. The joint PDF can be multimodal, in particular if several NLOS measurements exist and their prior probabilities are not known accurately. Further measurements are used to update the PDF and the position is estimated from the maximum a posteriori. Their approach has the advantage of including probabilistic information about the LOS/NLOS states of the signals. They highlight that the performance, in a simulation environment, depends on the number of detected signals.

All these publications evaluate the proposed methods in simulations. Kim *et al.* (2001) provide experimental results of a position method in an urban environment, using CDMA signals. They use a two-stage Kalman filter: a first filter estimates the signal biases and a second filter calculates the position after correction for the biases. The authors report errors of about 300 m at the beginning of the experiment and under 50 m after 3 min of tracking.

Two methods to mitigate non-line-of-sight effects

We consider the user of a mobile device, such as a smartphone, who wants to know his/her horizontal position as quickly as possible, even if the device has just been turned on. This approach is sometimes called “snapshot” or “push-to-fix” in contrast to position tracking, for which the measurements are accumulated and the user position is continuously tracked. We set the maximum latency of the position calculation to 500 ms.

The device makes the measurements and calculates the position, without assistance from network equipment. One of the methods presented by Caffery *et al.* (1998a) requires angle-of-arrival information from the base stations, which may only be possible with assistance from the network. It is also possible that the position is calculated on a network server and may then be transmitted back to the user. This approach is taken by some of the methods developed for the E-911 mandate, when the computing power of the user device is too limited.

The position is estimated from the iterative least-squares algorithm presented in Chapter 2. The position equation is simpler than for GPS signals: the transmitters are static, hence calculating the time of transmission of the signals is not required and a two-dimensional position can be determined from at least three measurements. The code period of the pilot signal, T_{pilot} , is longer than the GPS L1 C/A signal and this almost guarantees the convergence of the algorithm if the initial position is known within 8000 km and the dilution of precision is reasonable. We assume the pseudorange measurements have additive white Gaussian noise of standard deviation 60 m, and the measurements are independent between BTSs. The iterative algorithm is stopped when the square root of the sum of the squared residuals becomes smaller than 0.1 m. The initial position is set within 1.5 km of the true position, which could be provided using RSS or Cell-ID positioning for instance.

Most BTSs only cover a sector of about 120° and they are grouped by three, with different identifiers, to cover a cell. I ignored the angular information about the user position contained in the coverage of the BTSs, although it could improve the position accuracy by constraining the solution inside a cellular sector.

Most of the algorithms for NLOS mitigation are not able to work within the snapshot scenario we are interested in, as they require measurements collected over longer periods of time. We investigate two of the methods that do not require such filtering:

- the *residual rejection* algorithm is an ad-hoc method mentioned in Cong *et al.* (2004), among others. It consists of iteratively calculating the position, rejecting the measurement whose residual is the largest and above a given threshold, and repeating until all the measurement residuals are below the rejection threshold. I chose a threshold of 3σ , where σ is the standard deviation of the measurement noise; and
- the *full enumeration* of all the combinations of measurements, developed by Pi-Chun Chen (1999).

Some algorithms, such as the one designed by Wylie-Green *et al.* (2001), estimate the probability of a signal being a LOS, NLOS, or a false alarm. I believe this method is the most appropriate for positioning with NLOS signals, since it embeds the uncertainty on the propagation models. However, the classification of a signal can only be performed with enough measurements and a good prior position, which are not available in a snapshot scenario.

The full enumeration is particularly computationally demanding and is unlikely to be practical on a smartphone. It is, however, presented for completeness, since we

expect that it provides better results. Experiments will show that this method is actually inefficient and inaccurate.

We wish to give more weight to early signals when dealing with a set of TOA candidates from a same BTS, as in the all-peaks detector. I found that a useful heuristic was to change the variance of the measurement noise as a function of the order of arrivals of the detected paths. I used a simple linear function, where the first signal component was set to a measurement noise of 60 m of standard deviation, which increased for the following components by 30 m/ μ s.

Positioning results with outdoor and indoor signals

The receiver's positions were calculated with indoor and outdoor measurements, for every possible combinations of NLOS mitigation algorithms and TOA estimators presented in the previous sections. The results are presented in Universal Transverse Mercator (UTM) coordinates projected on the WGS-84 ellipsoid. The sources of CDMA2000 measurements were the same as the ones used for the stability experiments presented in Section 5.2.

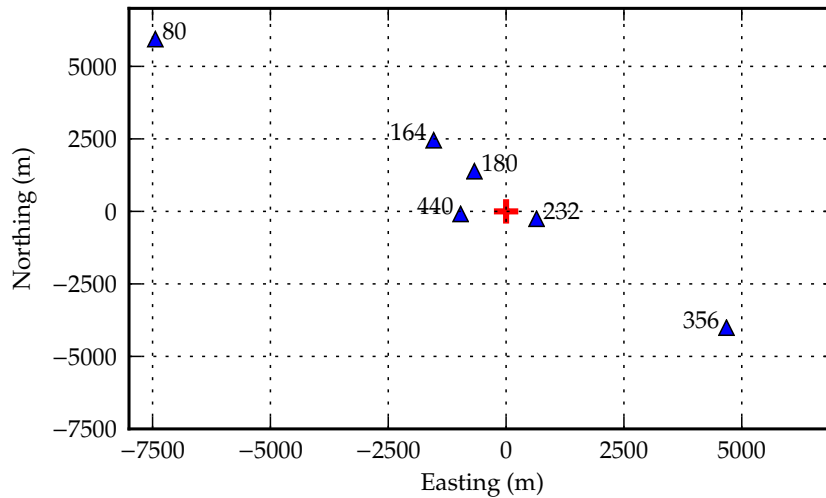


Figure 5.6: Map of the base stations (blue triangles) and the receiver (red cross) positions. The coordinates are in the UTM coordinate system and centred on the position of the receiver CDMA2000 antenna.

The transmitter geometry is represented in Figure 5.6. The vertical position of the antennas at the BTS was uncertain. Some antennas were located at the top of pre-existing buildings and others were attached on masts anchored at ground level. I used Google Maps (*Google Maps* 2012) to take the altitude of the base stations. The

heights of the centres of phase of the antennas, above ground level, were estimated from photographs. We can assume this leads to a systematic vertical error of about 100 m.

The Cramér-Rao bound of the position estimator is calculated from Equation 2.19 in Chapter 2, under the assumption that the signals from all seven BTSs have been detected. The noise variances of the pseudo-range measurements from the different BTSs are taken from the lower bounds calculated in Table 5.3. Fewer signals are detected when the antenna is indoors and the CRLB of the position estimate becomes wider.

Table 5.4: Statistics of the position errors using outdoor CDMA2000 signals. The circular error probable is calculated after the median bias has been removed from the position error; the CEP is relative to the median position estimated and not to the true position.

Multipath mitigation	TOA estimator	Filter	Median bias (m)	CEP _{50%} relative (m)	CEP _{90%} relative (m)
Residuals	Single-path	No	1	23	49
Residuals	Single-path	Median	1	15	32
Residuals	Heuristic	No	1	23	49
Residuals	Heuristic	Median	0	15	32
Residuals	SAGE	No	1	23	50
Residuals	SAGE	Median	0	15	32
Full enumeration	Single-path	No	3	46	164
Full enumeration	Single-path	Median	1	26	65
Full enumeration	Heuristic	No	4	46	173
Full enumeration	Heuristic	Median	2	27	67
Full enumeration	SAGE	No	1	46	172
Full enumeration	SAGE	Median	4	27	73

The position errors using outdoor signals are summarised in Table 5.4. I used the circular error probable (CEP) to analyse the position errors. Different definitions of the CEP may exist and I defined the CEP as the radius of the circle that included a given percentile of errors, after removal of the bias. The CEP_{50%} was for the median of the errors and the CEP_{90%} for the 90-percentile of the errors. I did not observe any significant bias. The circular error was between 20 m and 50 m and the median filter reduced this error to between 15 m and 30 m.

I then re-used the set of indoor measurements described in Section 5.2 to analyse the performance within an indoor environment. The true locations of these measurements were not known with an accuracy better than 10 m. I considered that the true position of the indoor antenna was the same as the one of the outdoor CDMA antenna, minus 6 m in height to reflect the location of the floor where the experiments were conducted.

The position errors presented in this section may thus have an error component caused by the uncertainty in the true position of the measurements, which is bounded by the largest dimension of building, about 20 m. The analysis still holds as the uncertainties in the true positions were dominated by the larger errors in the TOA estimations.

Table 5.5: Statistics of the position errors using indoor CDMA2000 signals. The circular error probable is calculated after the median bias has been removed from the position error; the CEP is relative to the median position estimated and not to the true position.

Multipath mitigation	TOA estimator	Filter	Median bias (m)	CEP _{50%} relative (m)	CEP _{90%} relative (m)
Residuals	Single-path	No	347	278	577
Residuals	Single-path	Median	417	262	506
Residuals	Heuristic	No	481	328	596
Residuals	Heuristic	Median	536	301	553
Residuals	SAGE	No	61	153	635
Residuals	SAGE	Median	33	121	589
Full enumeration	Single-path	No	20	222	1703
Full enumeration	Single-path	Median	74	185	693
Full enumeration	Heuristic	No	140	283	1043
Full enumeration	Heuristic	Median	167	223	827
Full enumeration	SAGE	No	78	249	≫ 10 km
Full enumeration	SAGE	Median	26	177	805

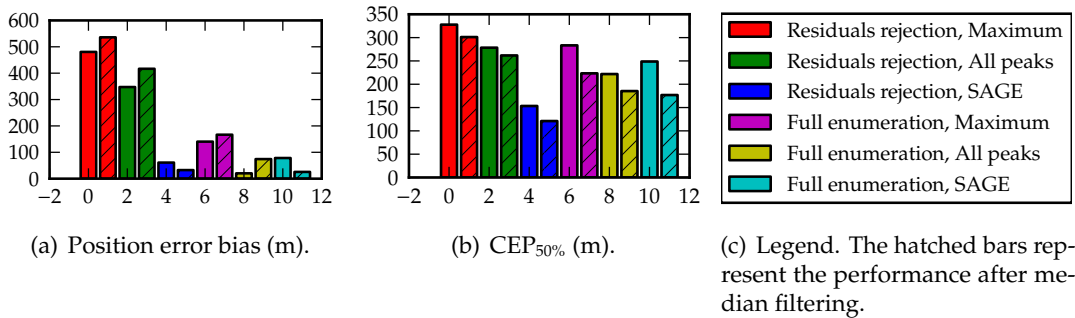
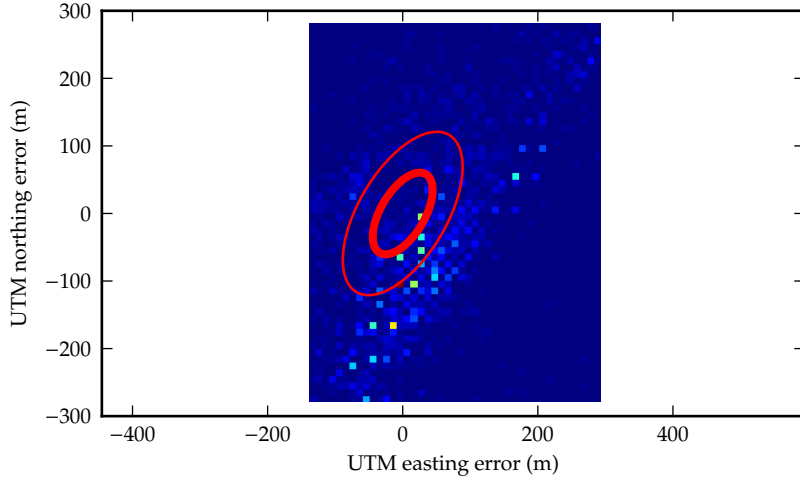
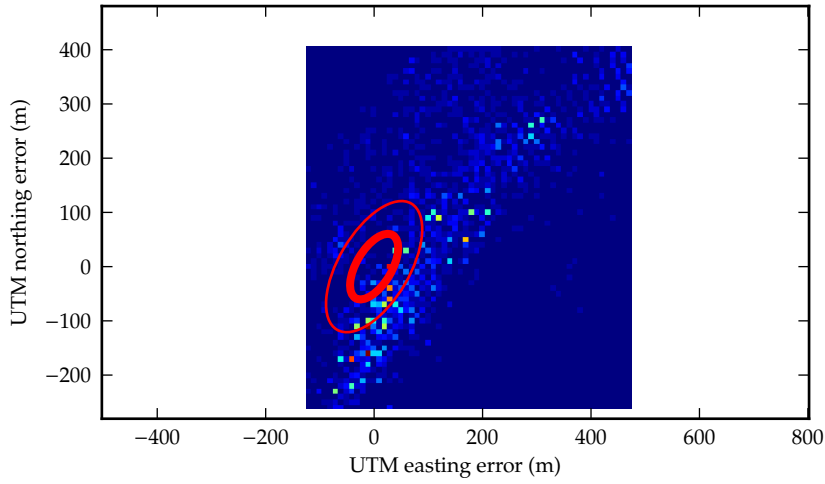


Figure 5.7: Summary of median position errors for all combinations of detectors and positioning methods.

The position errors using the indoor signals are summarized in Table 5.5 and Figure 5.7. The smallest bias was obtained for the full enumeration of all the peaks detected in the likelihood ratio. This combinatorial method was the most computationally expensive and it did not provide the best median error. A combination of SAGE estimation and residual rejection was the second-best method in terms of bias and it offered the smallest relative position errors. The median filter increased the bias error



(a) Residual rejection with SAGE detector.

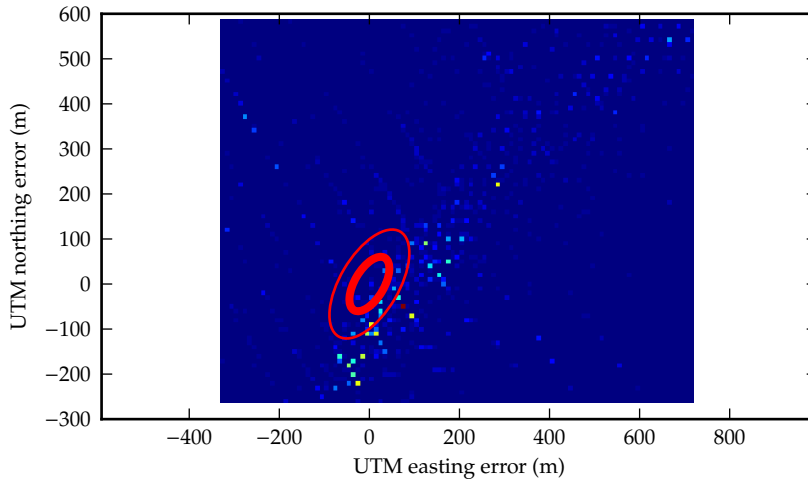


(b) Residual rejection with maximum detector.

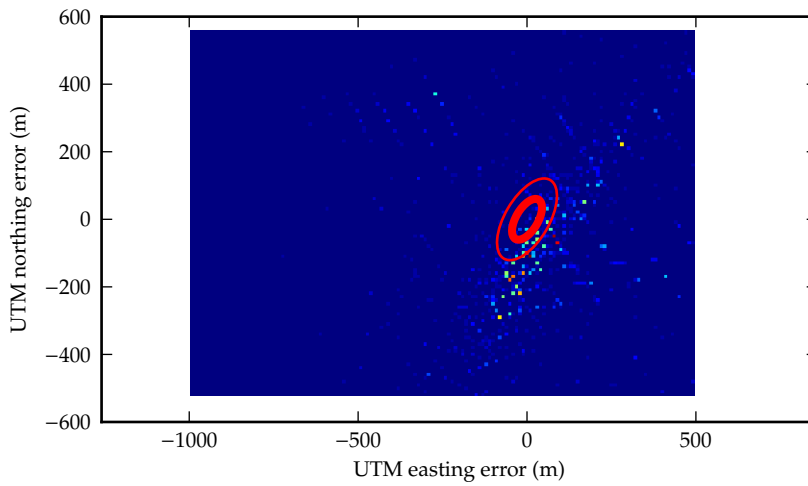
Figure 5.8: Position errors of indoor signals, presented as 2D-histograms, with rejection of measurements associated to large residuals. The colour of each cell indicates the frequency of the position solutions calculated inside the cell.

of all positions except when the SAGE estimator was used. A possible reason is that the position estimate was systematically biased because of the NLOS signals. The median operation reduced the estimator variance, as shown by the smaller median error, but did not improve the estimator bias.

Figures 5.8 and 5.9 show that the shapes of theoretical CRLB curves are in good agreement with the observed errors. We also note that the positions errors with the full



(a) Full enumeration with maximum detector.



(b) Full enumeration with SAGE detection.

Figure 5.9: Position errors of indoor signals, presented as 2D-histograms, using the full enumeration of measurement combinations. The colour of each cell indicates the frequency of the position solutions calculated inside the cell.

enumeration methods concentrated in a few discrete locations, whereas the residual rejection method had a more even error distribution.

Conclusions

The SAGE-based estimator combined with a residual rejection method provided the best position accuracy and computational efficiency for my series of measurements. The

position error at 50% was about 20 m with no bias using outdoor signals. As expected, indoor positioning with CDMA2000 signals was more challenging. A systematic bias of about 60 m was observed and the position accuracy, corrected for the bias, was about 150 m at the 50-percentile. It is unlikely that the systematic bias, introduced by the NLOS signals, can be corrected in a snapshot scenario, even with more sophisticated algorithms. Tracking of the measurements over a longer period of time is required to gather more information about which signals are LOS or NLOS.

5.6 Positioning using GNSS and cellular signals

This section presents the evaluation of a positioning algorithm that combines GPS and CDMA2000 signals.

Challenges of GNSS and cellular signals combining

Combining the times of arrival of the CDMA2000 and GPS measurements is straightforward since the two systems are synchronised together. The GPS measurements can provide additional pseudo-range measurements that can be included in the position equation. This approach has several advantages.

We have seen in the previous section that the detection of CDMA2000 signals can be challenging indoors and three measurements are not always available. The added signals improve the least-squares solution, both in terms of accuracy and availability.

Furthermore, signals in an indoor environment with one entry point, such as a window, can have a large range of signal strengths. In CDMA systems, this can introduce the near-far problem, since the noise floor at the receiver input is increased by the spread-spectrum modulation of the stronger signals, which mask the more attenuated signals. I did not observe the near-far problem in these experiments since the receiver had a large dynamic range. However, this can be problematic in mass-market mobile receivers and it can reduce the number of base stations available for positioning.

Another advantage of using GPS measurements is that it adds diversity to the propagation conditions of the signals. GPS signals typically arrive from high elevations, whereas CDMA2000 ones generally propagate in a horizontal plane. The GPS signals thus add some vertical components to the problem geometry. The GPS signals may also be less affected by multipath propagation, although this depends on their angles of arrivals. The GPS L1 C/A signal has a bandwidth of about 20 MHz, compared with 1.2288 MHz for CDMA2000. Wider bandwidths improve the TOA estimation and may be beneficial to mitigate multipath errors. However, most mass-market GPS receivers

have a narrower bandwidth, generally around 2 MHz, and the L1 C/A signal is not designed for precise positioning. It is therefore unlikely that the wider bandwidth of GPS signals be a source of a performance improvement.

A drawback of assisted-GNSS receivers with millisecond-ambiguity positioning, described in Section 2.5, is the need to estimate the signal transmission times, which adds another unknown variable to the position equation. This may be a problem for the availability of positioning in indoor environments, where enough signals may not be detected. However, CDMA2000 networks are synchronised with GPS time, hence the mobile device knows an approximation of the GPS system time. The only uncertainty in the GPS system time is related to the unknown propagation time of the CDMA2000 signal carrying the GPS time. I will show that the time information provided by the CDMA2000 network is accurate enough to calculate the times of transmission of the GPS signals, thus removing one unknown variable from the position equation.

The method presented in this section might be similar to the Hybrid-AFLT system commercialised under the name *gpsOne*[™] by Qualcomm Inc. Biacs *et al.* (2002) give some general information about this system, however most of the details seem proprietary. Other research on the fusion of cellular and GNSS signals includes Mensing *et al.* (2010), who present simulation results of positioning using a combination of GPS and cellular 4G LTE signals. Their method includes signal tracking to improve the position solution over time and does not address NLOS mitigation.

Extraction of GPS time from CDMA2000 data

The CDMA2000 BTSs transmit the times of their clocks in the Synch Channel Messages (SCHM), as described in 3GPP2 (2004b, §3.7.2.3.2.26). The time resolution of this message is 80 ms and its transmission is aligned with the transmission of the pilot code. The SCHM also carries information about the base station identification, the PN offset index, and the carrier frequency. I describe my implementation of the SCHM decoder in Appendix B.

Positioning with pseudo-range combining

I now derive the position equation combining the CDMA2000 and GPS signals. The full GPS pseudo-ranges can not be calculated since the GPS signals are too weak to allow decoding of the navigation data. Only fractional measurements, with an ambiguity of the period of the L1 C/A code, $T_{CA} = 1$ ms, are available. The solution to this problem

is given by the millisecond-ambiguity method introduced in Section 2.5, which seeks to resolve the full pseudo-range of the signals and determine the satellite positions.

The first step is to resolve the millisecond ambiguity in the L1 C/A signals, which requires knowing the GPS system time with an accuracy better than $500\text{ }\mu\text{s}$ at the receiver location. The maximum range of BTS is about 15 km, about $50\text{ }\mu\text{s}$, and we have seen the CDMA2000 signals are synchronised with the GPS time with an accuracy of about $2\text{ }\mu\text{s}$. The GPS time, from the CDMA2000 Sync Channel Message, is thus known at the receiver location with enough accuracy to resolve the millisecond ambiguity.

The second step is to calculate the time of transmission (TOT) of the L1 C/A signal in order to determine the satellite positions. The time of transmission is calculated from the time-of-week word of the navigation data in a receiver with tracking loops. This information is not available to our high-sensitivity receiver and the time of transmission must be estimated by the receiver. This requires an additional unknown variable to estimate this time. However, the CDMA2000 Sync Channel Message can provide the GPS time with an uncertainty which is caused only by the unknown propagation time and is bounded by a maximum error of $50\text{ }\mu\text{s}$. The maximum range rate of the GPS is about 465 m/s , therefore the pseudo-range error caused by the uncertain satellite position is less than 0.023 m , which is perfectly acceptable in our application. This eliminates the need for an additional unknown variable, thus making more measurements available to solve the position equation. The satellite ephemeris is downloaded from the International GNSS Service (see Dow *et al.*, 2009).

The position equation needs to be altered since the signals, although synchronised, have spreading codes with different periods. We consider a set of $i = 1, \dots, N_{\text{tx}}$ transmitters, sending positioning signals with possibly different periods. The time relationships between the code periods and the propagation times are represented schematically in Figure 5.10, with: TOT_i , the time of transmission of the signal from transmitter i ; TOR_i , the time of reception of the signal; t_0 , the time origin of the receiver time scale; and t_{align} , the last time at which all the positioning codes were aligned. The goal is to calculate the true, unknown, range $\|\mathbf{x}_i - \mathbf{x}\|$. We neglect the clock bias of the transmitters, which can be simply applied as a correction to TOR. From the diagram, we can deduce the following relationships:

$$\begin{aligned}
 \|\mathbf{x}_i - \mathbf{x}\| &= \text{TOR}_i - \text{TOT}_i \\
 &= \underbrace{(\text{TOR}_i - t_0)}_{\text{code phase}} + \underbrace{(t_0 - \hat{t}_0)}_{\text{local time error}} + \underbrace{(\hat{t}_0 - t_{\text{align}})}_{\text{new local time origin}} - \underbrace{(\text{TOT}_i - t_{\text{align}})}_{\text{code period ambiguity}} \quad (5.2) \\
 &= \hat{t}_i - b_u + \hat{t}_0 \bmod T_{\text{lcm}} - k_i T_i
 \end{aligned}$$

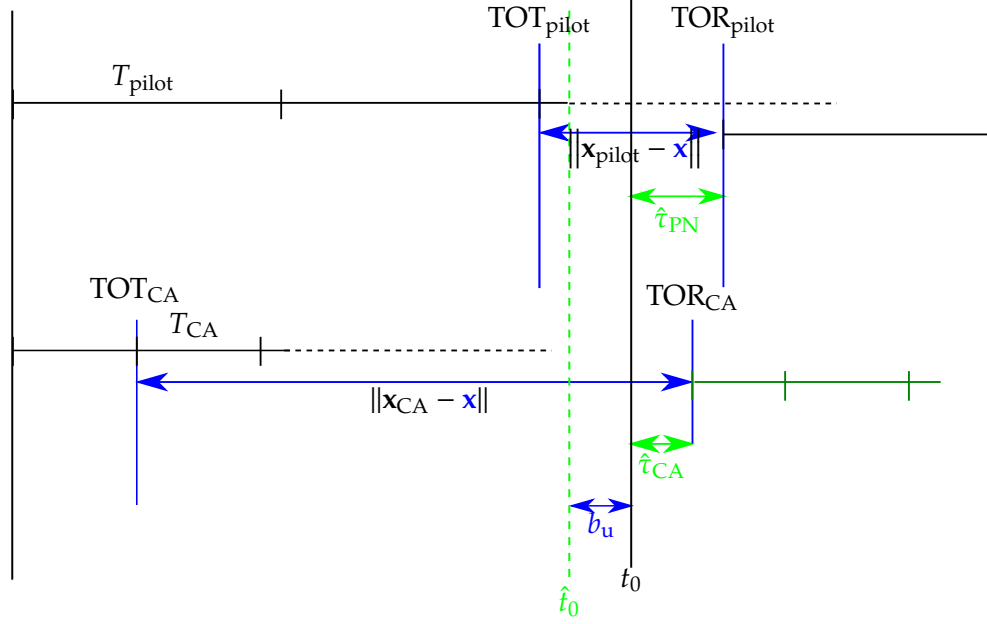


Figure 5.10: Timing diagram of CDMA2000 and GPS synchronisation signals. The unknown variables are represented in green and the measurements in blue. The subscripts pilot and CA are used to label the variables related to the CDMA2000 and GPS systems, respectively.

with

- T_i , the code period of the signal from transmitter i ;
- \hat{t} , the measured code phase;
- b_u , the unknown receiver time bias;
- T_{lcm} , the shortest period that all the ranging codes have in common;
- \hat{t}_0 , an estimate of the GPS system time at the beginning of the measurements; and
- k_i , the unknown integer number of code periods since the latest instant when the signals were aligned.

The position equation, Equation 5.2, is similar to the position equation with millisecond-ambiguity positioning presented in Chapter 2, except that the receiver bias b_u is substituted by the corrected bias $(b_u - \hat{t}_0) \bmod T_{\text{lcm}}$. Formally, $T_{\text{lcm}} = \text{LCM}(T_{\text{CA}}, T_{\text{pilot}})$ where $\text{LCM}(x, y)$ is the least common multiple of x and y . For the GPS L1 C/A and CDMA2000 PN pilot signals, we have $T_{\text{lcm}} = 80$ ms. \hat{t}_0 is required with an accuracy better than the smallest signal code period in order to resolve k_i unambiguously. We showed this was possible in the previous section, using the CDMA2000 system time given in the Sync Channel Message.

Indoor GPS signal acquisition

Detecting the synchronisation parameters of indoor signals requires long signal integration periods. Agarwal *et al.* (2002) highlight the importance of maximising the length of the coherent integration period in order to maximise the probability of detection, although this increases the search space size and the acquisition time, as seen in Chapter 3. We can, however, effectively reduce the search space since we have fine-time aiding from the CDMA2000 network. The larger search space caused by the finer resolution is thus balanced by a smaller total size, hence the time-to-first-fix can remain the same.

The bit flips of the navigation message limit the coherent integration time to a maximum of 20 ms for the GPS L1 C/A signal. Advanced high-sensitivity techniques, such as the ones described by Ziedan (2006), can extend the coherent integration time beyond the length of one navigation bit, although this generally requires computationally-demanding algorithms. Fine-time aiding makes these methods more tractable. The full pseudorange is available with fine-time aiding, hence the bit edges can be estimated within a few hundreds of microseconds, depending on the initial uncertainties about the receiver time and position. It then becomes possible to correct the phase shifts introduced by the navigation message and extend the coherent integration time, a technique often called “data wipe-off”. I did not perform any data wipe-off because some of the experiments were carried out while walking. The changing Doppler frequencies caused by the human motion would have decreased the sensitivity of the receiver using long coherent integration times.

I chose a coherent integration time of 3 ms, which may not be optimal but provides reasonable performance for this evaluation. The result of the coherent integration was squared and 330 further non-coherent integrations were performed, resulting in a total integration time of 990 ms. This integration time provided a near-certain probability of detection for signal strengths down to 24 dB-Hz, using a threshold set for a false-alarm rate of 10^{-4} . I noticed the noise floor at the input of the GPS indoor channel varied with the location of the indoor antenna. I disabled the automatic gain control of the signal analyser and used an adaptive threshold in order to keep a constant false-alarm rate. I chose an FFT-based acquisition of the GPS signals, as explained in Chapter 2, which used the full code-phase search space. The range of possible codes phases was 0 to 1 ms and the resolution was given by the sample rate. The frequency offset was calculated from the approximate receiver position, the known bias of the local oscillator, and the approximate GPS system time provided by the CDMA2000 network. The search space

was thus composed of one frequency offset and 10 000 possible code phases.

Results of indoor positioning

The time biases of the times of arrival of the PN pilot signals were calibrated in Section 5.3 to ensure their synchronisation with GPS time. This calibration was performed using the SAGE estimator and I only employed this estimator in the rest of this section. Combining GPS and CDMA2000 signals required perfect synchronisation of the time scales of both systems, hence I applied the same estimator for both the calibration and the experiment. I only investigated the combination of indoor signals since the performance using only CDMA2000 outdoor signals was already satisfactory.

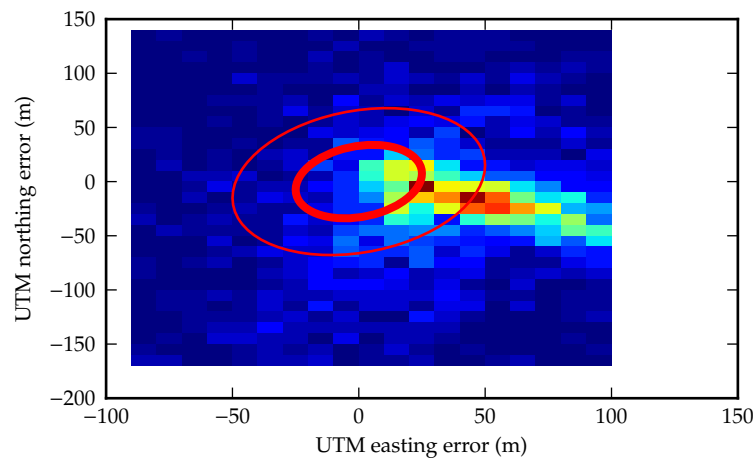


Figure 5.11: 2D-histogram of the position errors with indoor signals, CDMA2000 and GPS combining, with SAGE detector and residuals rejection.

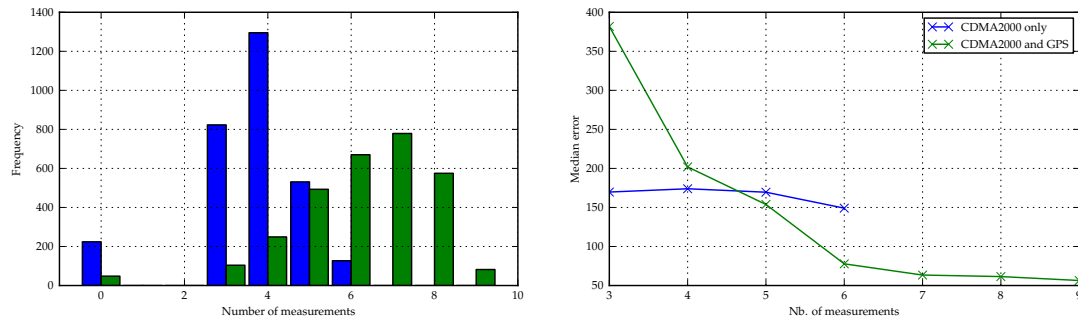
Table 5.6: Error statistics of positioning with CDMA2000 and GPS signals, indoors.

Multipath mitigation	TOA estimator	Filter	Median bias (m)	CEP _{50%} relative (m)	CEP _{90%} relative (m)
Residuals	SAGE	No	11	64	282
Residuals	SAGE	Median	12	54	204

The histogram of the position errors is presented in Figure 5.11 and the error statistics are summarised in Table 5.6. The performance of positioning using a combination of CDMA2000 and GNSS signals was approximately three times better than positioning using CDMA2000 signals only: the bias was reduced from about 30 m to about 10 m, and the CEP_{50%} was reduced from about 150 m to about 50 m.

5.7 Discussion

Indoor positioning improvement with signal combining



(a) Histogram of the number of measurements effectively used by the position algorithm. The blue bars represent the CDMA2000 measurements only and the green bars the combination of GPS and CDMA2000 signals.

(b) Effect of the number of measurements on the position error. The green curve includes all types of measurements, it does not attempt to match the CDMA2000 measurements with those used for the blue curve.

Figure 5.12: Comparison of the availability and accuracy between CDMA2000-only positioning and CDMA2000 and GPS combining.

Combining CDMA2000 and GPS signals improved the accuracy of the positioning when indoors, as well as the availability. Tables 5.5 and 5.6 show that the position error had a systematic bias of 61 m and a median relative error of 153 m with only CDMA2000 measurements, whereas the bias reduced to 11 m and the median error to 64 m with both CDMA2000 and GPS signals when indoors.

Figure 5.12 shows the relationships between the number of measurements used to calculate a position and the position error. The number of detected signals was generally higher than the number of signals presented in Figure 5.12, but some of the detected measurements were rejected by the NLOS positioning algorithms if they introduced large residuals. The median error of CDMA2000-based positioning was almost independent of the number of measurements used. This may have been related to the presence of a strong multipath component on BTS 440, which was included in almost all calculations. Although the position accuracy with three measurements did not seem to be improved by adding GPS signals, the three measurements were more likely to come from GPS signals, which had a poor geometry. The probabilities of detection of some of the GPS signals were higher than those of the CDMA2000, possibly because the signals from the satellites were less affected by multipath fading than the signals from the BTSs.

The set of indoor measurements was composed of sequences taken on two different

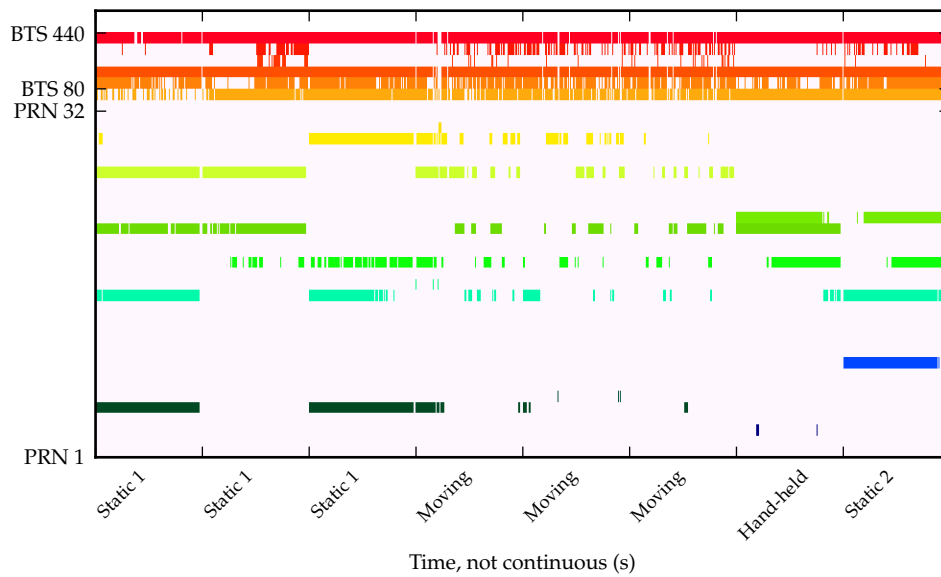


Figure 5.13: Signal detection indoors. The different sequences of measurements are juxtaposed in the diagram, hence the time scale is not continuous. The “Static1” and “Moving” sequences were performed on a same day, whereas the “Hand-help” and “Static2” experiments were carried out on a different day.

days, as seen in Section 5.2. The total duration of the experiment during each day was about 10 minutes, which was short enough to neglect the changes in the GPS constellation geometry. However, it was difficult to summarise the results for both days, since the geometry changed between these days. I analysed the geometry of the transmitters for the first day of measurement only. The high-sensitivity receiver generally detected 4 to 5 satellites successfully when the receiver was static. An exhaustive analysis of the geometry of the transmitters and its effects on the DOP were difficult since we used an algorithm that could reject some transmitters at every time step. The varying sets of transmitters meant the DOP was not constant. Figure 5.13 shows the evolution of the measurements used by the positioning algorithm for the different series of experiments. We note that the detection and use of the signals from the BTSs were generally constant. On the other hand, the acquisition of GPS signals was more difficult when the antenna is moving. The coherent integration time of 3 ms was not a limiting factor as the antenna was moved slowly and the Doppler shift remained small. It is more likely that the multipath fading reduced the GPS signal strength too much to ensure a reliable acquisition at every time step.

The horizontal dilution of precision (HDOP) is frequently used to relate the root mean squared of the position errors and the geometry of the transmitters. The relationship

between the root mean squared and the $\text{CEP}_{50\%}$ is linear and, for a bivariate normal, we have the $\text{RMS} = 1.2\text{CEP}_{50\%}$ see Diggelen, 2007. The HDOP can therefore be also used to compare the 50% CEP. However, the dilution of precision assumes a Gaussian noise on the pseudo-range measurement, which is not the case in our experiments because of the NLOS signals. Besides, the sample root mean squared of the position errors is affected by a few outliers and can not be computed accurately.

The comparison between HDOPs may therefore be unreliable. However, it may help coarsely quantify the contribution of the geometry to the improvement in the position error we observed between the two experiments. The HDOP for the CDMA2000 transmitter geometry was 1.89 and it was 1.06 for the CDMA2000 and GPS transmitters geometry, taking the four GPS satellites that were the most frequently detected. The inclusion of the GPS signals should therefore have reduced the standard deviations of the position errors by about 43%, simply by improving the number of transmitters and their geometry. Instead, we observed a 60% improvement in the $\text{CEP}_{50\%}$, thus showing that the addition of GPS satellites had more benefits than we could expect from the theoretical performance.

Non-line-of-sight mitigation in snapshot receivers

We have only addressed the case of snapshot receivers, for which only 500 ms worth of measurements is available. Figure 5.5 shows that the durations of the fades, also called the coherence time of the channel, was typically of a few seconds for the measurements made on a static receiver indoors. The duration of the measurements used by the snapshot receiver was thus not long enough to identify and filter the non-line-of-sight components.

Multipath mitigation algorithms that exploit measurements taken over durations longer than the coherence time of the channel are examples of time diversity techniques. An alternative to time diversity is space diversity, which exploits the differences in the propagation characteristics of a channel at different locations. Space diversity is commonly used in radio communication systems to mitigate the effects of multipath fading. Dietrich *et al.* (2001) show that combining the signals received from two antennas often provide an average gain of 10 dB above the signal at one antenna only. Space diversity thus mitigates the effect of multipath fading, which can improve the detection of indoor signals in a fading channel. I have not had the opportunity to try space diversity techniques, however I expect that the detection rate of the signals when walking with the antenna, shown in Figure 5.13, would be significantly higher. The

higher detection rate would give more pseudo-range measurements to the positioning algorithm and thus improve the position accuracy.

Most multi-antenna receivers used in positioning systems perform more advanced processing than simply combining the signals. Antenna arrays have been used in GNSS receivers to measure the angles of arrival of the signals, which can be used to identify jamming signals for example. More importantly, determining the angles of arrival of the signals can help identify the non-line-of-sight components. Broumandan *et al.* (2008) have performed measurements on a CDMA2000 network and used the MUSIC super-resolution algorithm to identify the NLOS signals. Their results suggest that the antenna array is particularly beneficial in situations where few pseudo-range measurements, typically three, are available. However, the space required for an antenna array with more than two antennas is often not compatible with hand-held devices, as the antennas must be separated by about the wavelength of the radio-frequency carrier.

Positioning with accurate clocks

Further research could exploit the accuracy of clocks to improve the signal acquisition performance, a remark that was also made in Chapter 4. The time accuracy of the CDMA2000 signals enables the receiver to know the bit edges of the navigation message. This opens the way to using coherent integration times that are longer than the code period of the PN signal, which improves the sensitivity of the receiver. I also mentioned that direct-position estimation techniques, as proposed by Closas *et al.* (2007) and Axelrad *et al.* (2011), must deal with the addition of the local oscillator bias to the search space. Accurate time thus reduces the search space and facilitates the computation of the position directly from the received signals.

5.8 Conclusions

In summary, it is difficult to address the performance degradation caused by non-line-of-sight signals in a snapshot receiver. The most common mitigation methods assume that tracking the signals is possible and the accumulation of measurements help identify and mitigate the NLOS conditions. A snapshot receiver only has a few milliseconds worth of measurements, which is often much shorter than the coherence time of a multipath channel, hence the NLOS conditions can not be identified. A more promising approach, for snapshot receivers, is to increase the number of signals employed by the positioning algorithm. I showed two methods in this chapter that can increase the number of signals available. The first method consists of combining measurements

from GNSS and cellular systems. The second method consists of using an accurate estimate of the GPS system time provided by the cellular network to remove one of the unknown variable in the position equation, thus increasing the availability of the solution to fewer measurements.

Conclusions

6.1 Summary of contributions

The work presented in this thesis focused on the use of GNSS receiver in cellular networks. As such, we have only considered a “push-to-fix” scenario, explained in Chapter 2, a situation which had not been addressed frequently in the literature. The main contributions of this work are both theoretical and experimental.

We have first seen, in Chapter 3, a new mathematical framework to calculate a lower bound of the time-to-first-fix of assisted-GNSS receivers. This work was based on the flow-graph method already proposed in the literature, but which was limited to the mean acquisition time of a single satellite. The framework consists in a flexible collection of several mathematical tools, such as the probability generating function, that can be reused to model the acquisition process of different types of GNSS receivers. I applied these tools to the case of an assisted-GPS receiver and I studied the impact of a fading channel on the acquisition time. One of the results is that the TTFF can be significantly improved by the presence of a single strong signal, a phenomenon which is not observed in non-assisted receivers. The lower bound also provides some insight about the expected performance of a receiver, which can be useful during the testing and verification of receivers.

Chapter 4 contained the results of experiments about the time stabilities of the synchronisation signals in GSM networks. The results showed a large heterogeneity in the stabilities of the signals from different base stations. Some base stations had a stability better than a few microseconds over several days, while other had variations of hundreds of milliseconds within one day. However, the measurements showed that the

base stations were synchronised neither between themselves, nor with an external time reference. They were therefore not capable of providing universal time information, which is required in order to provide time assistance to a GNSS receiver. I developed an ensemble filter which maintains a single estimate of the universal time by exploiting the time stability of the GSM synchronisation signals. The absolute time of the filter was periodically updated by calculating the GPS position and time. The results, using a set of twelve base stations in Cambridge, UK, showed that such a filter can provide fine-time aiding with an accuracy better than $10\text{ }\mu\text{s}$.

The case of synchronised network was addressed in Chapter 5, where I report the results of experimental on a CDMA2000 network. The CDMA2000 standard specifies that the network clocks must be synchronised within $2\text{ }\mu\text{s}$ of the GPS time, but the standard does not specify the stability. The measurements showed that the CDMA2000 network I considered was both stable and accurately synchronised with the GPS time. The synchronisation and the stability were then exploited to derive pseudo-range measurements from the times-of-arrival of the CDMA2000 pilot signals. The user's position was calculated with a median circular error of about 20 m in an outdoor environment. The non-line-of-sight measurements degraded the performance in an indoor environment, even after applying a mitigation algorithm, and the indoor position had a bias of about 60 m and a median relative error of 150 m. The pseudo-range measurements from the CDMA2000 base stations were combined with the fractional pseudo-ranges from the GPS satellites, which were typically used in mobile devices that require a short time-to-first-fix. I detailed how the position equation can be solved when using pseudo-noise signal of different code periods. Both the accuracy and the availability were significantly improved by the addition of GPS measurements.

6.2 Future work

Different points of the methods developed in this thesis could be improved in future works. For example, a more accurate model of false alarms in flow-graph methods could be investigated. The results presented in Chapter 3 could be compared with the performance of simpler filter, median or moving average filters for instance. All these improvements require more detailed assumptions about the receiver structure, cellular network architectures, user expected performance and trade-offs, etc. that are beyond the scope of this thesis, but that could be discussed in a follow-up work focused on the practical implementation details.

Third and fourth-generation cellular networks, for example W-CDMA and LTE,

have larger signal bandwidths, thus offering more possibilities of multipath mitigation.

A promising research area is the joint positioning approach proposed by Closas *et al.* (2007) and Axelrad *et al.* (2011). The most common acquisition methods of GNSS signals, which we have seen in this thesis, has two steps: first, the maximum-likelihood estimates of the synchronisation parameters are calculated using a GLRT, then the position is calculated from the synchronisation parameter estimates. On the other hand, joint positioning is a one-step method, where the likelihood function of the user's position is calculated directly from the observed signals. The signals are thus combined together and even weak signals, below the detection threshold of a classical GLRT detector can contribute to the position solution. This approach has not been used commercially yet, possibly because it is more computationally demanding and because classical methods work well in good conditions. However, I think that GNSS receivers could benefit from joint positioning, in particular in challenging situations such as operating with weak signals in multipath conditions. One of the problems with joint positioning is that the search space of the unknown parameters, the three spatial coordinates and the user bias, is larger than the search space of the synchronisation parameters used in the classical approach. The work on fine-time aiding presented in this thesis could help reduce the search space by providing an accurate estimate of the user clock bias. The search space of the joint positioning solution can even become smaller than the search space of a multi-constellation receiver. Joint positioning may also resolve some problems caused by multipath propagation, since it requires the full likelihood function of the pseudo-range, not simply the most likely value of the pseudo-range. The multipath components that appear in the likelihood function of one signal can therefore be partially reduced by the likelihood values of another signal.

GPS software receiver

The GPS software receiver designed and used throughout this thesis is presented in this section. The software receivers used to receive the GSM and CDMA2000 signals were very similar to the one presented here.

A.1 Acquisition

A schematic representation of the acquisition stage of the GPS receiver is shown in Figure A.1.

The input signal was sampled at baseband with a period T_s and a block of N_s complex samples was acquired. The samples acquired are represented by the vector \mathbf{z} . The signal was first down-converted to remove the frequency offset, f , caused by the Doppler effect and the local oscillator bias.

The coherent integration period was T_{coh} and it was a multiple of the code period, T_{CA} , of the GPS L1 C/A signal, such that $T_{\text{coh}} = N_{\text{coh}} T_{\text{CA}}$. The sampling period, T_s was

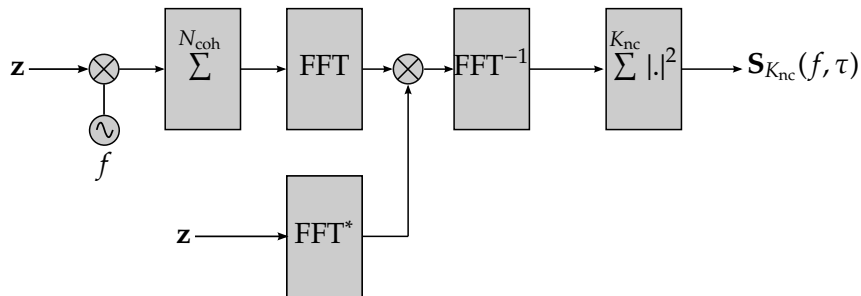


Figure A.1: Block diagram of the software GPS receiver.

chosen such that there was an integer number of samples, N_{CA} , in a code period. The sampling period was also chosen so that N_{CA} was a power of two (or at least close to a power of two), in order to use the optimised fast Fourier transform implementation of the DFT.

The linearity property of the discrete Fourier transform allowed us to perform the coherent integration before removing the code phase. The length of the DFT was thus kept to N_{CA} samples, which made it easier to optimise the implementation of the FFT. Signal vectors of length N_{CA} were added together N_{coh} times to form the vector of integrated signal \mathbf{z}_{coh} . The receiver architecture was optimised by setting the number of samples acquired, N_s , such $N_s = N_{coh}N_{CA}$.

The acquisition was performed following the fast Fourier transform (FFT) method proposed by Davenport (1991). This method exploits the dual relationship between the circular correlation and the product operation when using the discrete Fourier transform. The advantage was that the FFT, with a computational complexity of $O(N \log_2 N)$, was more computationally efficient than the correlation operation, which has a complexity of $O(N^2)$. The FFT was implemented using the FFTW library.

A vector composed of the N_{CA} samples of discrete Fourier transform of the C/A code, \mathbf{z}_{CA} , was stored for the duration of the acquisition. The conjugate of the correlation vector was then multiplied with the results of the FFT of the input vector after coherent integration. The value of the log-likelihood ratio was calculated by squaring the magnitude of the vector of correlated samples. The result of this operation formed the output values of $S_0(\tau, f)$, which was calculated for a fixed f and for all the discrete code phases calculated by the FFT. The acquisition process was repeated for another frequency offset candidate, f , at a distance Δf of the previous frequency offset.

The correlator output, $S_1(\tau, f)$, was thus calculated with a resolution of Δf along the frequency-offset axis, and with a resolution of T_s along the code-phase axis. It is worth pointing out that the FFT approach calculates the correlation values for all the code-phase values in the discrete search space. The FFT does not scale well when only the values for a subset of the code phase search space are required.

A.2 Tracking

The frequency offset estimate, \hat{f} , was tracked using a phase-locked loop (PLL) and the code-phase estimate, $\hat{\tau}$, was tracked using a delay-locked loop (DLL). The frequency offset was first refined using a frequency estimator similar to the one described by Borio *et al.* (2008a). This estimator also provided the phase offset of the signal. The phase

offset and the improved frequency estimate helped the convergence of the phase-locked loop. The code-phase estimate was already accurate enough for the good operation of the DLL.

The tracking loops were implemented using the C programming language and were optimised using look-up tables of the trigonometric functions and vectorised functions from the Basic Linear Algebra Subprograms (BLAS) library. The frequency estimate from the acquisition stage was refined by using a frequency estimator, which helped the convergence of the PLL. We only require off-line, not real-time, operation of the receiver hence the synchronisation parameters of the different signals were tracked sequentially. The values of the code phase, frequency offset, and carrier phase estimated by the tracking loops were then stored on disk for further processing.

CDMA2000 Sync Channel Message

The CDMA2000 standard is complex and understanding the reference documents can be time consuming. This appendix contains the information relevant to the decoding of the Sync Channel Message, from the encoding of the physical layer to the structure of the information in the bitstream.

B.1 Physical channel

The physical layer is described in the document 3GPP2 C.S0002. The logical channel F-SYNC is formed by successively applying the following operations:

1. convolutional encoding of rate $k = 2$, with the polynomials 753 (octal) and 561 (octal);
2. symbol repetition of rate 2;
3. block interleaving of length 128 symbols, based on a bit reversed-order permutation table;
4. symbol mapping at a rate of 4800 bit/s and spreading by the Walsh sequence 32, at a rate of 1.2888 Mc/s;
5. spreading by the IS95 pilot pseudo-noise code, shifted by the index offset of the base station; and
6. modulation using binary phased-shift keying and pulse shaping.

The demodulation is performed by correlation with the conjugate of the PN sequence, despreading by the Walsh sequence, coherent integration to recover the 128 symbols at a rate of 4800 bit/s, de-interleaving using the permutation table, further coherent integration to remove the symbol repetition, and finally convolutional decoding using the Viterbi algorithm.

The Walsh sequence 32 is equal to the 32nd row of the Hadamard matrix of order 64. In this case, the Walsh sequence, represented as a non-return-to-zero (NRZ) signal, is simply a succession of 16 bits +1, followed by 16 bits -1, i.e. $\{+1, \dots, +1, -1, \dots, -1\}$. This pattern is a common property of the $n/2$ row of any n -order Hadamard matrix.

B.2 Frames and super-frames

The next step is to recover the F-SYNC channel frames, as described in the 3GPP2 C.S0003 and C.S0004 documents. One frame is composed of 32 bits, the first bit being the Start Of Message bit (SOM) and the remaining 31 bits are the data bits.

Three frames form of *super-frame*, and an integer number of super-frames form a message *capsule*. A message capsule always starts by a frame where the SOM bit is set to one. All the SOM bits are removed from the frames and only the data bits are assembled to form the data bits of the capsule.

The capsule carries data packets with the following format, described in C.S0004:

- bits 0 to 7 contain the Packed Data Unit (PDU) length (MSG_LENGTH), in bytes;
- bits 8 to 15 contain the message type, composed of 2 bits for the Protocol Descriptor (PD) and 6 bits for the message ID (MSG_ID).
- bits 16 until MSG_LENGTH bytes contain the PDU;
- at the end of the PDF, 30 bits are used for by the Cyclic Redundancy Check (CRC) value; and
- after the CRC bits, a variable number of bits with value 0 are used to pad the capsule to the size an integer number super-frames.

On the F-SYNC channel, the Sync Channel Message is assigned the MSG_ID tag SCHM, of value binary value 000001.

B.3 Sync Channel Message structure

Finally, the content of the Sync Channel Message is described in 3GPP2 C.S0005 (section 3.7.2.3.2.26 of revision D). Of interest are:

- the NID and SID fields contain the network and the base station identifiers;
- the PILOT_PN field contains the base station offset of the PN code;
- the SYS_TIME field contains the system time (defined to be GPS time), with a resolution of 80 ms;
- some other fields contain the number of leap seconds, time zone offset and daylight saving time;

- the CDMA_FREQ field contain the frequency of the base station, using the CDMA frequency code described in 3GPP2 C.S0057;
- other fields contain protocol revision information, spreading rate information, etc.

References

- 3GPP. *3GPP - LTE*. 3GPP LTE website. URL: <http://www.3gpp.org/LTE> (visited on 28/11/2012) (cit. on pp. 30, 136).
- (July 2003a). *Multiplexing and Multiple Access on the Radio Path*. TS 05.02. 3rd Generation Partnership Project (3GPP) (cit. on p. 98).
 - (Sept. 2003b). *Radio subsystem synchronization*. TS 05.10. 3rd Generation Partnership Project (3GPP) (cit. on pp. 98, 134).
 - (Dec. 2004). *Physical layer on the radio path; General description*. TS 05.01. 3rd Generation Partnership Project (3GPP) (cit. on pp. 96, 97).
 - (Feb. 2005a). *Channel coding*. TS 05.03. 3rd Generation Partnership Project (3GPP) (cit. on p. 98).
 - (Nov. 2005b). *Radio Transmission and Reception*. TS 05.05. 3rd Generation Partnership Project (3GPP) (cit. on p. 96).
- 3GPP website. *3GPP - Specifications*. URL: <http://www.3gpp.org/specifications> (visited on 08/11/2012) (cit. on p. 29).
- 3GPP2 (Dec. 1999). *C.S0010-0 Recommended Minimum Performance Standards for cdma2000 Spread Spectrum Base Stations* (cit. on p. 136).
- (Feb. 2004a). *C.S0002-D Physical Layer Standard for cdma2000 Spread Spectrum Systems* (cit. on pp. 136, 138).
 - (Feb. 2004b). *C.S0005-D Upper Layer (Layer 3) Signaling Standard for cdma2000 Spread Spectrum Systems* (cit. on p. 167).
 - (Mar. 2004c). *C.S0022-A Position Determination Service for cdma2000 Spread Spectrum Systems* (cit. on p. 157).
- Abate, J. and W. Whitt (Jan. 1992). "The Fourier-series method for inverting transforms of probability distributions". In: *Queueing Systems* 10 (1-2), pp. 5–87 (cit. on p. 66).
- Abdi, A., K. Wills, H. Barger, M.-S. Alouini and M. Kaveh (2000). "Comparison of the level crossing rate and average fade duration of Rayleigh, Rice and Nakagami fading models with mobile channel data". In: *Vehicular Technology Conference, 2000. IEEE VTS-Fall VTC 2000. 52nd*. Vehicular Technology Conference, 2000. IEEE VTS-Fall VTC 2000. 52nd. Vol. 4, 1850–1857 vol.4 (cit. on p. 70).
- Agarwal, N. *et al.* (Dec. 2002). "Algorithms for GPS operation indoors and downtown". In: *GPS Solutions* 6 (3), pp. 149–160 (cit. on p. 170).
- Akopian, D. and J. Syrjärinne (Oct. 2009). "A Fast Positioning Method Without Navigation Data Decoding for Assisted GPS Receivers". In: *Vehicular Technology, IEEE Transactions on* 58 (8), pp. 4640–4645 (cit. on p. 132).
- Alexander, S. (1983). "Characterising buildings for propagation at 900 MHz". In: *Electronics Letters* 19 (20), p. 860 (cit. on p. 18).

- Allan, D. (1966). "Statistics of atomic frequency standards". In: *Proceedings of the IEEE* 54 (2), pp. 221–230 (cit. on p. 102).
- Anghileri, M., M. Paonni, S. Wallner, J.-A. Ávila-Rodríguez and B. Eissfeller (Jan. 2010). "Performance Assessment of GNSS Signals in Terms of Time to First Fix for Cold, Warm and Hot Start". In: *Proceedings of the 2010 International Technical Meeting of The Institute of Navigation*. San Diego, CA, pp. 1051–1066 (cit. on pp. 68, 86).
- Axelrad, P., B. K. Bradley, J. Donna, M. Mitchell and S. Mohiuddin (2011). "Collective Detection and Direct Positioning Using Multiple GNSS Satellites". In: *Navigation* 58 (4), pp. 305–321 (cit. on pp. 52, 175, 179).
- Bahl, P. and V. Padmanabhan (2000). "RADAR: An in-building RF-based user location and tracking system". In: *INFOCOM 2000. Nineteenth Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE*. Vol. 2, 775–784 (cit. on p. 19).
- Bastide, F., O. Julien, C. Macabiau and B. Roturier (Feb. 2001). "Analysis of L5/E5 Acquisition, Tracking and Data Demodulation Thresholds". In: *Proceedings of the 15th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GPS 2002)*, pp. 2196–2207 (cit. on p. 61).
- Berger, J. O. (Aug. 1985). *Statistical Decision Theory and Bayesian Analysis*. 2nd. Springer (cit. on pp. 37, 44).
- Biacs, Z., G. Marshall, M. Moeglein and W. Riley (Sept. 2002). "The Qualcomm/SnapTrack Wireless-Assisted GPS Hybrid Positioning System and Results from Initial Commercial Deployments". In: *Proceedings of the 15th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GPS 2002)*, pp. 378–384 (cit. on p. 167).
- Blom, H. and Y. Bar-Shalom (1988). "The interacting multiple model algorithm for systems with Markovian switching coefficients". In: *Automatic Control, IEEE Transactions on* 33 (8), pp. 780–783 (cit. on p. 118).
- Borio, D., L. Camoriano, L. Lo Presti and M. Fantino (2008a). "DTFT-based frequency lock loop for GNSS applications". In: *Aerospace and Electronic Systems, IEEE Transactions on* 44 (2), pp. 595–612 (cit. on p. 182).
- Borio, D., L. Camoriano and L. Lo Presti (2008b). "Impact of GPS acquisition strategy on decision probabilities". In: *Aerospace and Electronic Systems, IEEE Transactions on* 44 (3), pp. 996–1011 (cit. on p. 71).
- Borre, K., D. Akos, N. Bertelsen, P. Rinder and S. Jensen (2007). *A Software-Defined GPS and Galileo Receiver*. Birkhäuser Boston (cit. on p. 50).
- Bregni, S. and L. Barbieri (Dec. 2003). "Experimental evaluation of the impact of network frequency synchronization on GSM quality of service during handover". In: *Global Telecommunications Conference, 2003. GLOBECOM '03. IEEE*. Vol. 6, 3457–3461 vol.6 (cit. on p. 99).
- Broumandan, A., T. Lin, J. Nielsen and G. Lachapelle (Sept. 2008). "Practical Results of Hybrid AOA/TDOA Geo-Location Estimation in CDMA Wireless Networks". In: *Vehicular Technology Conference, 2008. VTC 2008-Fall. IEEE 68th. Vehicular Technology Conference, 2008. VTC 2008-Fall. IEEE 68th*, pp. 1–5 (cit. on p. 175).
- Brown, K. R. J. (Sept. 1991). "The Theory of the GPS Composite Clock". In: *Proceedings of the 4th International Technical Meeting of the Satellite Division of The Institute of Navigation*. ION GPS 1991. Albuquerque, NM, pp. 223–242 (cit. on p. 124).

- Brown, R. G. and P. Y. C. Hwang (1997). *Introduction to Random Signals and Applied Kalman Filtering with MATLAB Exercises*. Vol. 3rd ed. John Wiley & Sons, Inc. (cit. on pp. 42, 43, 103–105).
- Caffery, J. J. and G. Stuber (May 1998a). "Subscriber location in CDMA cellular networks". In: *IEEE Transactions on Vehicular Technology* 47 (2), pp. 406–416 (cit. on pp. 137, 159).
- Caffery, J. and G. Stuber (Apr. 1998b). "Overview of radiolocation in CDMA cellular systems". In: *Communications Magazine, IEEE* 36 (4), pp. 38–45 (cit. on p. 31).
- Cavers, J. K. (1978). "On the Fast Fourier Transform Inversion of Probability Generating Functions". In: *IMA Journal of Applied Mathematics* 22 (3), pp. 275–282 (cit. on pp. 66, 67).
- Chaffee, J. and J. Abel (Apr. 1994). "GDOP and the Cramer-Rao bound". In: *IEEE Position Location and Navigation Symposium, 1994.*, IEEE Position Location and Navigation Symposium, 1994, pp. 663–668 (cit. on p. 52).
- Chaffee, J. (Nov. 1987). "Relating the Allan Variance to the Diffusion Coefficients of a Linear Stochastic Differential Equation Model for Precision Oscillators". In: *Ultrasonics, Ferroelectrics and Frequency Control, IEEE Transactions on* 34 (6), pp. 655–658 (cit. on p. 105).
- Closas, P., C. Fernandez-Prades and J. Fernandez-Rubio (2007). "Maximum Likelihood Estimation of Position in GNSS". In: *Signal Processing Letters, IEEE* 14 (5), pp. 359–362 (cit. on pp. 52, 175, 179).
- Cong, L. and W. Zhuang (Mar. 2004). "Nonline-of-sight error mitigation in mobile location". English. In: *INFOCOM 2004. Twenty-third Annual Joint Conference of the IEEE Computer and Communications Societies*. INFOCOM 2004. Twenty-third Annual Joint Conference of the IEEE Computer and Communications Societies. Vol. 1. IEEE, p. 659 (cit. on pp. 159, 160).
- Corazza, G. E, C. Caini, A. Vanelli-Coralli and A. Polydoros (July 2004). "DS-CDMA code acquisition in the presence of correlated fading - Part I: theoretical aspects". English. In: *IEEE Transactions on Communications* 52 (7), pp. 1160–1168 (cit. on p. 91).
- Corazza, G. (1996). "On the MAX/TC criterion for code acquisition and its application to DS-SSMA systems". In: *Communications, IEEE Transactions on* 44 (9), pp. 1173–1182 (cit. on p. 71).
- Couronneau, N., P. Duffett-Smith and A. Mitelman (Jan. 2011). "Acquisition Time of the GPS L1 C/A Signal in an Indoor Environment". In: *Proceedings of the 2011 International Technical Meeting of The Institute of Navigation*. San Diego, CA, pp. 767–774 (cit. on p. 60).
- Dardari, D., A. Conti, U. Ferner, A. Giorgetti and M. Win (Feb. 2009). "Ranging With Ultrawide Bandwidth Signals in Multipath Environments". In: *Proceedings of the IEEE* 97 (2), pp. 404–426 (cit. on p. 41).
- Davenport, R. (1991). "FFT processing of direct sequence spreading codes using modern DSP microprocessors". In: *Aerospace and Electronics Conference, 1991. NAECON 1991., Proceedings of the IEEE 1991 National*. Aerospace and Electronics Conference, 1991. NAECON 1991., Proceedings of the IEEE 1991 National, 98–105 vol.1 (cit. on pp. 48, 182).
- Davis, J. A., C. A. Greenhall and P. W. Stacey (Feb. 2005). "A Kalman filter clock algorithm for use in the presence of flicker frequency modulation noise". In: *Metrologia* 42 (1), pp. 1–10 (cit. on p. 104).

- Dempster, A. P., N. M. Laird and D. B. Rubin (Jan. 1977). "Maximum Likelihood from Incomplete Data via the EM Algorithm". In: *Journal of the Royal Statistical Society. Series B (Methodological)* 39 (1). ArticleType: research-article / Full publication date: 1977 / Copyright © 1977 Royal Statistical Society, pp. 1–38 (cit. on p. 139).
- DiCarlo, D. and C. Weber (Aug. 1980). "Statistical Performance of Single Dwell Serial Synchronization Systems". In: *Communications, IEEE Transactions on* 28 (8), pp. 1382–1388 (cit. on p. 68).
- Dietrich C.B., J., K. Dietze, J. Nealy and W. Stutzman (Sept. 2001). "Spatial, polarization, and pattern diversity for wireless handheld terminals". In: *IEEE Transactions on Antennas and Propagation* 49 (9), pp. 1271–1281 (cit. on p. 174).
- Diggelen, F van (Jan. 2007). "GNSS Accuracy – Lies, Damn Lies and Statistics". In: *GPS World* 18 (1) (cit. on p. 174).
- Dow, J. M., R. E. Neilan and C. Rizos (Feb. 2009). "The International GNSS Service in a changing landscape of Global Navigation Satellite Systems". In: *Journal of Geodesy* 83 (3-4), pp. 191–198 (cit. on pp. 109, 168).
- Drane, C., M. Macnaughtan and C. Scott (Apr. 1998). "Positioning GSM telephones". In: *IEEE Communications Magazine* 36 (4), pp. 46–54, 59 (cit. on p. 31).
- Duffett-Smith, P. and R. Rowe (June 2001). "Comparative A-GPS and 3G-Matrix Testing in a Dense Urban Environment". In: Proceedings of the 19th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS 2006), pp. 3006–3011 (cit. on p. 31).
- Duffett-Smith, P. J and J. Craig (2004). "Matrix, and enhanced satellite positioning". English. In: *Fifth IEE International Conference on 3G Mobile Communication Technologies, 2004. 3G 2004. Fifth IEE International Conference on 3G Mobile Communication Technologies, 2004. 3G 2004. IET*, pp. 364–367 (cit. on pp. 31, 133).
- Duffett-Smith, P. J, P. Hansen, S. D Hern and A. R Pratt (Apr. 2007). "Atomic Quality Clocks for Cell-Phone GPS without the Atoms". In: Proceedings of the 63rd Annual Meeting of The Institute of Navigation, pp. 496–503 (cit. on p. 96).
- Duffett-Smith, P. J. and G. Woan (1992). "The CURSOR Radio Navigation and Tracking System". In: *The Journal of Navigation* 45 (02), pp. 157–165 (cit. on p. 18).
- Duffett-Smith, P. and M. Macnaughtan (May 2002). "Precise UE positioning in UMTS using cumulative virtual blanking". In: *3G Mobile Communication Technologies, 2002. Third International Conference on (Conf. Publ. No. 489). 3G Mobile Communication Technologies, 2002. Third International Conference on (Conf. Publ. No. 489)*, pp. 355–359 (cit. on p. 144).
- Elnahrawy, E., X. Li and R. Martin (Oct. 2004). "The limits of localization using signal strength: a comparative study". In: *2004 First Annual IEEE Communications Society Conference on Sensor and Ad Hoc Communications and Networks, 2004. IEEE SECON 2004. 2004 First Annual IEEE Communications Society Conference on Sensor and Ad Hoc Communications and Networks, 2004. IEEE SECON 2004*, pp. 406–414 (cit. on p. 19).
- ETSI website. ETSI GSM. URL: <http://www.etsi.org/website/technologies/gsm.aspx> (visited on 08/11/2012) (cit. on p. 29).
- European Union (Sept. 2012). *European GNSS (Galileo) Open Service Signal In Space Interface Control Document* (cit. on p. 27).

- Faragher, R. (Aug. 2007). "Studies of radio propagation in urban environments and the effects of multipath interference on positioning systems". Cambridge, UK: University of Cambridge (cit. on pp. 95, 96, 105, 116, 139).
- Faragher, R. and P. Duffett-Smith (Dec. 2010). "Measurements of the effects of multipath interference on timing accuracy in a cellular radio positioning system". In: *Radar, Sonar Navigation, IET* 4 (6), pp. 818–824 (cit. on pp. 116, 148).
- Faragher, R., C. Sarno and M. Newman (Apr. 2012). "Opportunistic radio SLAM for indoor navigation using smartphone sensors". In: *Position Location and Navigation Symposium (PLANS), 2012 IEEE/ION*. Position Location and Navigation Symposium (PLANS), 2012 IEEE/ION, pp. 120–128 (cit. on p. 22).
- Favey, E., D. Megnet, A. Rempfler and H. Mathis (May 2001). "Integration of a GSM Receiver with GPS for Integrated Navigation or for Quick Satellite Signal Acquisition". In: Proceedings of the 18th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS 2005), pp. 1425–1432 (cit. on pp. 95, 115).
- Fessler, J. and A. Hero (Oct. 1994). "Space-alternating generalized expectation-maximization algorithm". In: *IEEE Transactions on Signal Processing* 42 (10), pp. 2664–2677 (cit. on p. 139).
- Fischer, S., H. Grubeck, A. Kangas, H. Koorapaty, E. Larsson and P. Lundqvist (Sept. 1998). "Time of arrival estimation of narrowband TDMA signals for mobile positioning". English. In: *The Ninth IEEE International Symposium on Personal, Indoor and Mobile Radio Communications, 1998*. The Ninth IEEE International Symposium on Personal, Indoor and Mobile Radio Communications, 1998. Vol. 1. IEEE, 451–455 vol.1 (cit. on p. 158).
- Flcury, B., M. Tschudin, R. Heddergott, D. Dahlhaus and K. Ingeman Pedersen (Mar. 1999). "Channel parameter estimation in mobile radio environments using the SAGE algorithm". In: *IEEE Journal on Selected Areas in Communications* 17 (3), pp. 434–450 (cit. on p. 139).
- Galleani, L and P Tavella (June 2003). "On the use of the Kalman filter in timescales". In: *Metrologia* 40 (3), S326–S334 (cit. on p. 124).
- Gold, R. (1967). "Optimal binary sequences for spread spectrum multiplexing (Corresp.)". In: *Information Theory, IEEE Transactions on* 13 (4), pp. 619–621 (cit. on p. 26).
- Google Maps (Dec. 2012). URL: <https://maps.google.com/> (visited on 13/12/2012) (cit. on p. 161).
- GPS Joint Program Office (Dec. 2004). *Navstar Global Positioning System Interface Specification* (cit. on p. 27).
- Groves, P. D. (2011). "Shadow Matching: A New GNSS Positioning Technique for Urban Canyons". In: *The Journal of Navigation* 64 (03), pp. 417–430 (cit. on p. 21).
- GSM Association website. GSM | About Us. URL: <http://www.gsma.com/aboutus/gsm-technology/gsm/> (visited on 08/11/2012) (cit. on p. 29).
- Gumacos, C. (Mar. 1963). "Analysis of an Optimum Sync Search Procedure". English. In: *IEEE Transactions on Communications Systems* 11 (1), pp. 89–99 (cit. on p. 62).
- Gustafsson, F. and F. Gunnarsson (July 2005). "Mobile positioning using wireless networks: possibilities and fundamental limitations based on available wireless network measurements". In: *IEEE Signal Processing Magazine* 22 (4), pp. 41–53 (cit. on p. 30).
- Hann, K. (Mar. 2012). *LTE Stretches Synchronization to New Limis* (cit. on p. 100).

- Hashemi, H. (July 1993). "The indoor radio propagation channel". In: *Proceedings of the IEEE* 81 (7), pp. 943–968 (cit. on p. 20).
- Holmes, J. and Chang Chen (1977). "Acquisition Time Performance of PN Spread-Spectrum Systems". In: *Communications, IEEE Transactions on* 25 (8), pp. 778–784 (cit. on pp. 59, 62, 64, 67, 86).
- Holmes, J. K., N. Morgan and P. Dafesh (Sept. 2006). "Theoretical Approach to Determining the 95% Probability of TTFF for the P(Y) Code Utilizing Active Code Acquisition". In: *Proceedings of the 19th International Technical Meeting of the Satellite Division of The Institute of Navigation. ION GNSS 2006*. Fort Worth, TX, pp. 201–211 (cit. on pp. 66, 68, 78).
- Hopkins, P. (Aug. 1977). "A Unified Analysis of Pseudonoise Synchronization by Envelope Correlation". English. In: *IEEE Transactions on Communications* 25 (8), pp. 770–778 (cit. on pp. 59, 62).
- "IEEE Standard Definitions of Physical Quantities for Fundamental Frequency and Time Metrology—Random Instabilities" (2008). In: *IEEE STD 1139-2008*, pp. c1–35 (cit. on p. 103).
- Jan, S.-S. and Y.-C. Lin (2009). "A new multi-C/A code acquisition method for GPS". In: *GPS Solutions* 13 (4), pp. 293–303 (cit. on p. 84).
- Jaynes, E. T. (June 2003). *Probability Theory: The Logic of Science*. Ed. by G. L. Bretthorst. Cambridge University Press. 758 pp. (cit. on p. 35).
- Jones, E., T. Oliphant, P. Peterson and others (2001). *SciPy: Open source scientific tools for Python* (cit. on p. 117).
- Ju-Yong Do, M. Rabinowitz and P. Enge (July 2007). "Robustness of TOA and TDOA Positioning Under Suboptimal Weighting Conditions". English. In: *IEEE Transactions on Aerospace and Electronic Systems* 43 (3), pp. 1177–1180 (cit. on p. 50).
- Kalman, R. E. (1960). "A New Approach to Linear Filtering and Prediction Problems". In: *Transactions of the ASME—Journal of Basic Engineering* 82 (Series D), 35–45 (cit. on pp. 23, 42).
- Kasper, J. and C. Hutchinson (May 1978). "The Omega navigation system—An overview". In: *IEEE Communications Society Magazine* 16 (3), pp. 23–35 (cit. on p. 23).
- Kay, S. M. (1993). *Fundamentals of statistical signal processing: estimation theory*. Upper Saddle River, NJ, USA: Prentice-Hall, Inc. (cit. on pp. 35, 40, 41).
- Kim, W., G.-I. Jee and J. Lee (2001). "Wireless location with NLOS error mitigation in Korean CDMA system". In: *3G Mobile Communication Technologies, 2001. Second International Conference on (Conf. Publ. No. 477)*. 3G Mobile Communication Technologies, 2001. Second International Conference on (Conf. Publ. No. 477), pp. 134–138 (cit. on p. 159).
- Klukas, R. (Sept. 1997). "Cellular Telephone Positioning Using GPS Time Synchronization". In: *Proceedings of the 10th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GPS 1997)*, pp. 1405–1414 (cit. on pp. 30, 140).
- Lannelongue, S. and P. Pablos (June 1998). "Fast Acquisition Techniques For G.P.S. Receivers". In: *Proceedings of the 54th Annual Meeting of The Institute of Navigation*. Denver, CO, pp. 261–269 (cit. on p. 54).
- Leon, F. de and J. Marciano (Nov. 2006). "Application of MUSIC, ESPRIT and SAGE Algorithms for Narrowband Signal Detection and Localization". In: *TENCON 2006*.

- 2006 IEEE Region 10 Conference. TENCON 2006. 2006 IEEE Region 10 Conference, pp. 1–4 (cit. on p. 140).
- Li, W., W. Yao and P. Duffett-Smith (Jan. 2009). “Comparative Study of Joint TOA/DOA Estimation Techniques for Mobile Positioning Applications”. In: *6th IEEE Consumer Communications and Networking Conference, 2009. CCNC 2009*, pp. 1–5 (cit. on p. 140).
- Lohan, E.-S., A. Lakhzouri and M. Renfors (2004). “Selection of the multiple-dwell hybrid-search strategy for the acquisition of Galileo signals in fading channels”. In: *2004 IEEE 15th International Symposium on Personal, Indoor and Mobile Radio Communications (IEEE Cat. No.04TH8754)*. 2004 IEEE 15th International Symposium on Personal, Indoor and Mobile Radio Communications. Barcelona, Spain, pp. 2352–2356 (cit. on p. 62).
- Malte Spitz. *Malte Spitz: Your phone company is watching* | Video on TED.com (cit. on p. 30).
- Mehra, R. (Apr. 1970). “On the identification of variances and adaptive Kalman filtering”. English. In: *IEEE Transactions on Automatic Control* 15 (2), pp. 175–184 (cit. on p. 116).
- Mensing, C., S. Sand and A. Dammann (2010). “Hybrid Data Fusion and Tracking for Positioning with GNSS and 3GPP-LTE”. In: *International Journal of Navigation and Observation* 2010, pp. 1–12 (cit. on p. 167).
- Meyr, H. and G. Polzer (Dec. 1983). “Performance Analysis for General PN-Spread-Spectrum Acquisition Techniques”. In: *Communications, IEEE Transactions on* 31 (12), pp. 1317–1319 (cit. on p. 68).
- Mitelman, A., P.-L. Normark, M. Reidevall, J. Thor, O. Gröqvist and L. Magnusson (Sept. 2006). “The Nordnav Indoor GNSS Reference Receiver”. In: *Proceedings of the 19th International Technical Meeting of the Satellite Division of The Institute of Navigation. ION GNSS 2006*. Fort Worth, TX, pp. 2494–2502 (cit. on pp. 79, 106).
- Morley, C. (2003). *XmlRpc++* (cit. on p. 107).
- Murphy, K. P. (1998). *Switching Kalman Filters* (cit. on p. 118).
- Nakagami, M. (1960). “The m-distribution – A general formula of intensity distribution of rapid fading”. In: *Statistical Methods in Radio Wave Propagation*. Ed. by W. Hoffmann (cit. on p. 149).
- National Coordination Office for Space-Based Positioning, Navigation, and Timing (Sept. 2012). *GPS.gov*. URL: <http://www.gps.gov/> (visited on 15/09/2012) (cit. on p. 24).
- Neven, W., T. Quilter, R. Weedon and R. Hogendoorn (Aug. 2005). *Report on Wide Area Multilateration EATMP TRS 131/04* (cit. on p. 18).
- Newman, P. *et al.* (Nov. 2009). “Navigating, Recognizing and Describing Urban Spaces With Vision and Lasers”. In: *Int. J. Rob. Res.* 28 (11-12), 1406–1433 (cit. on p. 22).
- Nuttall, A. (1970). “Alternate forms for numerical evaluation of cumulative probability distributions directly from characteristic functions”. In: *Proceedings of the IEEE* 58 (11), pp. 1872–1873 (cit. on p. 66).
- O’Driscoll, C., M. Petovello and G. Lachapelle (Jan. 2008). “Software Receiver Strategies for the Acquisition and Re-Acquisition of Weak GPS Signals”. In: *Proceedings of ION NTM08* (cit. on p. 86).
- O’Driscoll, C. (2007). “Performance Analysis of the Parallel Acquisition of Weak GPS Signals”. Department of Electrical and Electronic Engineering, National University of Ireland (cit. on pp. 62, 66, 72).
- Ofcom (2012). *Ofcom | Facts & Figures*. URL: <http://media.ofcom.org.uk/facts/> (visited on 16/09/2012) (cit. on p. 28).

- O'Mahony, N., G. Lachapelle and C. C. Murphy (2011). "Simplifying the Performance Analysis of the SPRT for GPS Acquisition". In: *International Journal of Navigation and Observation* 2011, pp. 1–15 (cit. on p. 62).
- Pany, T. (2010). *Navigation Signal Processing for GNSS Software Receivers*. 1st ed. Artech House Publishers. 330 pp. (cit. on pp. 35, 39–41, 48, 72, 105).
- Parkinson, B. W. and J. J. Spilker (Jan. 1996). *Global Positioning System: Theory & Applications (Volume One)*. 1st. (AIAA) American Institute of Aeronautics & Astronautics (cit. on pp. 24, 26, 49, 50, 70, 147).
- Patel, P. and J. Holtzman (June 1994). "Analysis of a simple successive interference cancellation scheme in a DS/CDMA system". In: *IEEE Journal on Selected Areas in Communications* 12 (5), pp. 796–807 (cit. on p. 142).
- Pauluzzi, D. and N. Beaulieu (Oct. 2000). "A comparison of SNR estimation techniques for the AWGN channel". In: *IEEE Transactions on Communications* 48 (10), pp. 1681–1691 (cit. on p. 80).
- Pi-Chun Chen (1999). "A non-line-of-sight error mitigation algorithm in location estimation". English. In: *1999 IEEE Wireless Communications and Networking Conference, 1999. WCNC. 1999 IEEE Wireless Communications and Networking Conference, 1999. WCNC. IEEE*, 316–320 vol.1 (cit. on pp. 158, 160).
- Polydoros, A. and C. Weber (1984a). "A Unified Approach to Serial Search Spread-Spectrum Code Acquisition—Part I: General Theory". In: *IEEE Transactions on Communications* 32 (5), pp. 542–549 (cit. on pp. 62, 64, 66, 75, 86).
- (1984b). "A Unified Approach to Serial Search Spread-Spectrum Code Acquisition—Part II: A Matched-Filter Receiver". In: *Communications, IEEE Transactions on* 32 (5), pp. 550–560 (cit. on p. 62).
- Proakis, J. (Aug. 2000). *Digital Communications*. 4th ed. McGraw-Hill Science/Engineering/Math (cit. on p. 37).
- "Radio positioning systems" (Mar. 2003). Pat. 6529165. P. J. Duffett-Smith, J. P. Brice and P. Hansen (cit. on p. 18).
- "Radio positioning systems" (Apr. 2008). Pat. 7359719. P. J. Duffett-Smith, J. P. Brice and P. Hansen. U.S. Classification: 455/456.6 (cit. on p. 18).
- Rasmussen, C. E. (2006). "Gaussian processes for machine learning". In: MIT Press (cit. on p. 127).
- Riley, K. F., M. P. Hobson and S. J. Bence (2006). *Mathematical methods for physics and engineering*. Cambridge University Press. 1362 pp. (cit. on p. 64).
- Ristic, B., S. Arulampalam and N. Gordon (2004). *Beyond the Kalman Filter: Particle Filters for Tracking Applications*. en. Artech House. 326 pp. (cit. on p. 43).
- Russian Institute of Space Device Engineering (2008). *Global Navigation Satellite System GLONASS Interface Control Document* (cit. on p. 27).
- Saleh, A. and R. Valenzuela (Feb. 1987). "A Statistical Model for Indoor Multipath Propagation". In: *IEEE Journal on Selected Areas in Communications* 5 (2), pp. 128–137 (cit. on p. 149).
- Schmidt, R. (Mar. 1986). "Multiple emitter location and signal parameter estimation". In: *IEEE Transactions on Antennas and Propagation* 34 (3), pp. 276–280 (cit. on p. 30).
- Simon, M. K., M.-S. Alouini and S. Member (1998). "A Unified Approach to the Performance Analysis of Digital Communication over Generalized Fading Channels". In: *Proc. IEEE*, 1860–1877 (cit. on pp. 70, 90).

- Sirola, N. and P. Syrjärinne (2002). "Solving GPS time and position without navigation data". In: *Proceedings of the ENC-GNSS 2002* (cit. on p. 54).
- Stirling-Gallacher, R., A. Hulbert and G. Povey (1996). "A fast acquisition technique for a direct sequence spread spectrum signal in the presence of a large Doppler shift". In: *Spread Spectrum Techniques and Applications Proceedings, 1996., IEEE 4th International Symposium on. Spread Spectrum Techniques and Applications Proceedings, 1996., IEEE 4th International Symposium on. Vol. 1, 156–160 vol.1* (cit. on p. 84).
- Syrjärinne, J. (2000). "Time recovery through fusion of inaccurate network timing assistance with GPS measurements". In: *Information Fusion, 2000. FUSION 2000. Proceedings of the Third International Conference on. Information Fusion, 2000. FUSION 2000. Proceedings of the Third International Conference on. Vol. 2, WED5/3–WED510 vol.2* (cit. on p. 132).
- Thrun, S. *et al.* (June 2006). "Stanley: The Robot that Won the DARPA Grand Challenge". In: *Journal of Field Robotics* 23 (9). Ed. by W. Periodicals, pp. 661–692 (cit. on p. 22).
- "Transfer of calibrated time information in a mobile terminal" (Dec. 2010). Pat. 7852267. P. J. Duffett-Smith, A. R. Pratt and D. W. Bartlett. Granted (cit. on p. 96).
- Trevisani, E. and A. Vitaletti (Dec. 2004). "Cell-ID location technique, limits and benefits: an experimental study". In: *Sixth IEEE Workshop on Mobile Computing Systems and Applications, 2004. WMCSA 2004. Sixth IEEE Workshop on Mobile Computing Systems and Applications, 2004. WMCSA 2004, pp. 51–60* (cit. on p. 20).
- United States Coast Guard (1994). *Specification of the transmitted Loran-C signal*. Distributed to depository libraries in microfiche. Shipping list no.: 94-0699-M. Washington, DC: U.S. Dept. of Transportation, U.S. Coast Guard (cit. on p. 23).
- Van Dierendonck, A. J., J. B McGraw and R. G Brown (Nov. 1984). *Relationship Between Allan Variances and Kalman Filter Parameters* (cit. on pp. 103–105).
- van Diggelen, F. (2002). "Indoor GPS theory & implementation". In: *Position Location and Navigation Symposium, 2002 IEEE. Position Location and Navigation Symposium, 2002 IEEE, pp. 240–247* (cit. on pp. 61, 82).
- (Mar. 2009). *A-GPS: Assisted GPS, GNSS, and SBAS*. 1st ed. Artech House (cit. on pp. 50, 53, 54).
- Van Trees, H. L. (1968). *Detection, estimation, and modulation theory*. New York: Wiley (cit. on pp. 35, 44).
- Ward, P. W., J. W. Betz and C. J. Hegarty (2006). "Satellite Signal Acquisition, Tracking, and Data Demodulation". In: *Understanding GPS: Principles and Applications*. 2nd edition. Chapter 5: Artech House (cit. on p. 84).
- Wax, M. and T. Kailath (Apr. 1985). "Detection of signals by information theoretic criteria". In: *IEEE Transactions on Acoustics, Speech and Signal Processing* 33 (2), pp. 387–392 (cit. on p. 142).
- Weiss, A. and E. Weinstein (Apr. 1983). "Fundamental limitations in passive time delay estimation—Part I: Narrow-band systems". In: *IEEE Transactions on Acoustics, Speech and Signal Processing* 31 (2), pp. 472–486 (cit. on p. 41).
- Wylie-Green, M. P and S. S Wang (2001). "Robust range estimation in the presence of the non-line-of-sight error". English. In: *Vehicular Technology Conference, 2001. VTC 2001 Fall. IEEE VTS 54th. Vehicular Technology Conference, 2001. VTC 2001 Fall. IEEE VTS 54th. Vol. 1. IEEE, 101–105 vol.1* (cit. on pp. 158, 160).

- Yong-Hwan Lee and Seung-Jun Kim (Nov. 2000). "Sequence acquisition of DS-CDMA systems employing Gold sequences". English. In: *IEEE Transactions on Vehicular Technology* 49 (6), pp. 2397–2404 (cit. on p. 62).
- Ziedan, N. I. (2006). *GNSS Receivers for Weak Signals*. Boston, Mass: Artech House. 234 pp. (cit. on p. 170).
- Ziv, J. and M. Zakai (May 1969). "Some lower bounds on signal parameter estimation". In: *IEEE Transactions on Information Theory* 15 (3), pp. 386–391 (cit. on p. 41).
- Zucca, C. and P. Tavella (Feb. 2005). "The clock model and its relationship with the Allan and related variances". In: *Ultrasonics, Ferroelectrics and Frequency Control, IEEE Transactions on* 52 (2), pp. 289–296 (cit. on pp. 104, 105).