Technische Fakultät
Albert-Ludwigs-Universität, Freiburg

Lehrstuhl für Kommunikationsysteme
Prof. Dr. Gerhard Schneider

Master thesis

Mobile Assisted GPS Localization in GSM Networks

July 9, 2012

Supervised by
M.Sc. Konrad Meier
M.Sc. Dennis Wehrle

First Examiner
Prof. Dr. Gerhard Schneider

Second Examiner
Prof. Dr. Christian Schindelhauer

Refik Hadžialić

Erklärung

Hiermit erkläre ich, dass ich diese Abschlussarbeit selbständig verfasst habe, keine anderen als die angegebenen Quellen/Hilfsmittel verwendet habe und alle Stellen, die wörtlich oder sinngemäß aus veröffentlichten Schriften entnommen wurden, als solche kenntlich gemacht habe. Darüber hinaus erkläre ich, dass diese Abschlussarbeit nicht, auch nicht auszugsweise, bereits für eine andere Prüfung angefertigt wurde.

Ort, Datum
(Place, Date)

Unterschrift
(Signature)

Acknowledgment

I would like to thank my supervisors Konrad Meier and Dennis Wehrle for their encouraging talks during the thesis. Things which have not been done before are intellectually seductive in a way. Beside the help from the supervisors I would like to thank my family and friends who supported me through my master studies, and the entire Communication systems department for their support, free coffee and to Prof. Dr. Gerhard Schneider for making all the required hardware available. I would like to thank Sebastian Schmelzer for his LaTeX tips, Michael Neves Pereira and Jonathan Bauer for borrowing me their cell phones to test my system with and Johan Latocha for patiently explaining me words I did not understand in the German language. I would like to thank Richard Zahoransky for the helping discussions.

Contents

1. Introduction

1.1. Motivation

Recent developments in the field of physics, chemistry and electronics have led to cheap and compact size manufacturing of diverse single chip integrated solutions. As a consequence of the rapid development it became possible to integrate a GPS receiver into almost every cell phone without dramatically and drastically increasing the price, physical size or weight of the cell phone. It is important to note, the number of wireless connections increased as well, in 2011 there were 6 billion mobile connections worldwide [19]. In the following European countries, Germany, France, Spain, Italy and UK, 44% of all GSM users own a smart phone, whereas in the US and Canada this number is slightly higher, 46% [16]. By the statistics of the Blur group 47% of all the cell phones on the world will be smart phones by 2015 [7].

An emerging new market of location based services (LBS) has grown out of it and since then changes the telecommunication and marketing industry with fast pace. In 2009, 63 million users used some of the LBS on their cell phones, this number is expected to grow in 2012 to 468 million users worldwide [7]. As social networks grow like Facebook, Twitter or Foursquare (a location based social network), it has become a trend for the users to share their location with their friends [7]. It has been reported that LBS represent a Bonanza opportunity for new startup companies [31]. New ideas and algorithms for tracking, navigation solutions, safety, security, local business search and payments will emerge from it as well as the new market that will emerge from the results of data mining user's movement [31]. The Enhanced 911 (E911), an emergency service in the US for linking emergency callers with appropriate public service (police, firefighters and emergency room), regulated with the US Federal Communication Commission (FCC) a standard for all telecommunication providers to have capabilities of localizing their users within a defined range [39]. Similar standards exist for Europe's E112 service as well [29]. Next generation networks, long term evolution (LTE) 4G networks, have been designed to have LBS capability integrated in the system and better LBS accuracy than compared to GSM networks [37]. In the introductory chapter, some of the most known positioning techniques

in wireless networks will be discussed and analysed, Cell-ID, time of arival, angle of arival and GPS positioning. Then the author will proceed and describe the goals of his thesis.

1.2. Related work

fit into small devices as smart [43]

1.3. Goals of the thesis

The goal of the following thesis is to: - implement the Radio Resource Location Protocol inside of OpenBSC, to the extent of delivering correct GPS assistance data to cell phone subscribers inside the GSM network - test the protocol on 5-10 different smart phones - describe and analyse the background processes taking place inside of the cell phone

2. GPS & Assisted-GPS

What use is knowledge if there is no understanding?

(Stobaeus)

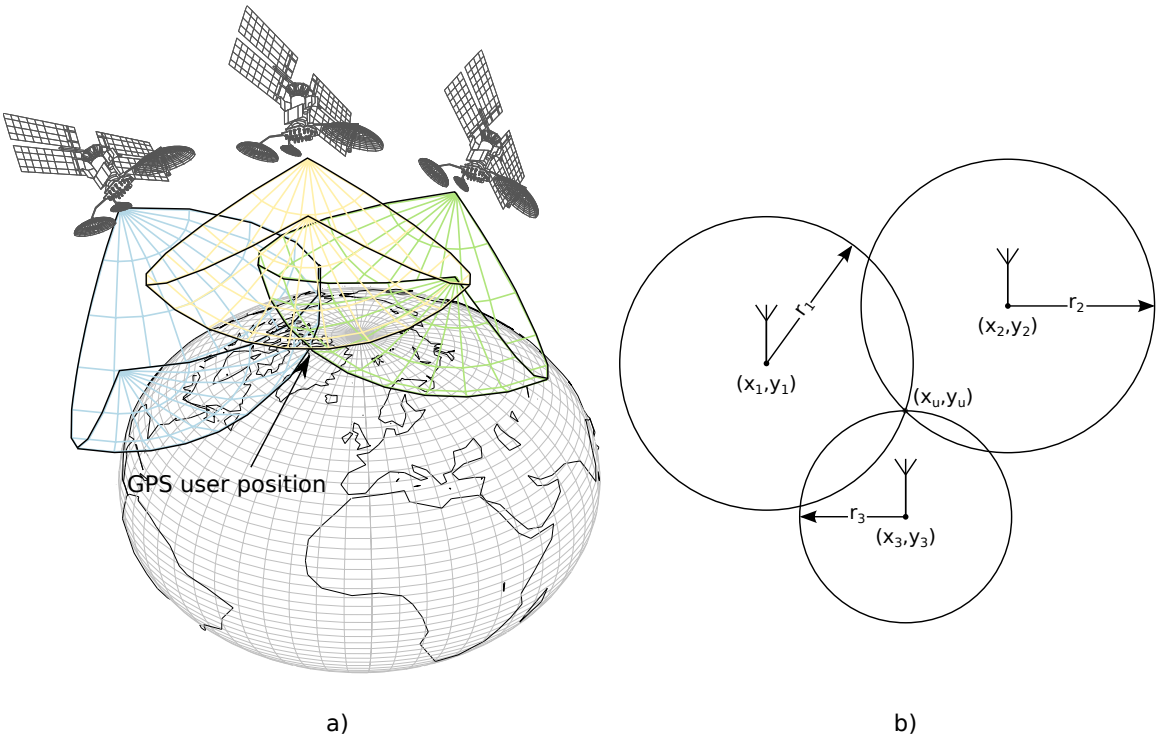

Figure 2.1.: GPS Simple working principle, a) example in 3D space with spheres b) example in 2D space with circles.

In the new global economy age, GPS positioning has become of important value for various services and businesses. It has been growing at a rate of 30% in the past few years and the application market is expected to be worth €240 milliard by 2020 only in Europe [17]. The goal of this chapter is to bring more details and insights of how GPS receivers work. The chapter is divided in few sections that explain how

the data are modulated before transmission, demodulated on the receiver, how the search space works, how the target user position is estimated and the errors that can influence the overall working of the system.

In this paragraph the general idea will be given how GPS works and how the position is estimated. Before all the details are revealed in the following sections, it is important to understand the basic principle of GPS navigation. GPS positioning works by using the principle of *trilateration*. Distances from the satellites to the GPS receiver are measured and from these distances receiver's position is estimated. The distances are estimated by measuring the signal propagation time between the satellites and the receiver, this position estimation technique is also known as time-of-arrival (TOA) method. Once sufficient amount of measurements from different satellites were generated, the position of the receiver can be approximated. It is important to understand that the positions from the satellites need to be known and same location reference system has to be used. The general principle of this idea can be seen in figure 2.1, picture (a) represents the idea with spheres in 3D space and picture (b) the same idea but in 2D space. The blue, yellow and green wireframes below the GPS satellites represent the spheres for a given range, between the satellite and the estimated position of the GPS user for the given satellite. By intersecting all the three spheres, the position of the user is estimated. In the next sections this general idea will be developed in more details, step by step, and the ideas will be verified using the appropriate mathematical models.

2.1. GPS data and signal modulation

The aim of this section is to give the reader an overview of the transmitted GPS data and to understand what type of processing takes place on the GPS satellite itself. As mentioned in the paragraph earlier, to estimate the position of the GPS receiver, it is important to know the position of the satellite at the moment of signal transmission. Prior to releasing the data in the athmosphere, they need to be modulated in order for the GPS receiver to receive and demodulate them.

Each one of the GPS satellites transmits the same type of information. The transmitted data are called *frames* [8]. One frame of data can be seen in figure 2.2. Every of the 25 transmitted frames can be divided into five subframes of 300 bits length [12]. The data in the frames are called *navigation data* because using them the GPS receiver can estimate user's position. Each subframe can be divided into

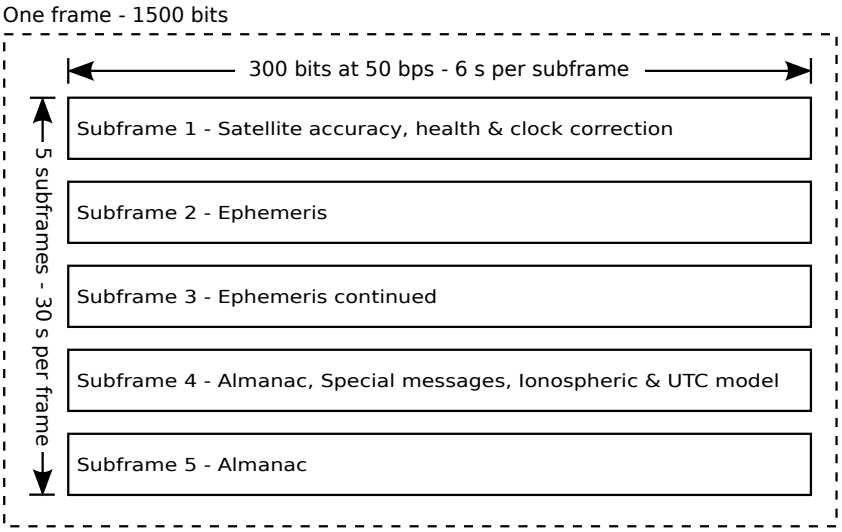

Figure 2.2.: One frame of 1500 bits on L1 frequency carrier

three fields of data, as shown in figure 2.3, telemetry (TLM), handover (HOW) word and rest of the data (navigation data). TLM is the first word of the subframe and consists of a unique preamble used to synchronize and identify the subframes [8]. HOW is the second word of the subframe and consists of the *GPS system time* and subframe ID [8]. GPS system time is the time the atomic clock on the satellite generates at the moment of subframe broadcast and it acts as a time stamp [2]. The third segment of the subframe, indicated as rest of data in figure 2.3, consists of the navigation data. The first subframe includes data about the satellite accuracy and health as well as parameters used for the clock corrections on the receiver side.

More details on these parameters will be given in section 2.2. Subframe two and three are made of *ephemeris data*. Ephemeris information are precise parameters for predicting the precise orbital position of the GPS satellite. Using ephemeris data for the specific system time stamp and the equations given in appendix section C the GPS receiver can precisely estimate the position (x_s, y_s, z_s) of the satellite. The first three subframes are satellite dependent and do not change in the transmitted 25 frames beside the system time stamp [1]. Fourth and fifth subframes include *almanac*

Figure 2.3.: Subframes always start with telemetry and handover words

data, low-precision clock corrections, ionospheric model and UTC time calculation parameteres. Almanac information are rough coarse parameters for predicting the orbital position of the GPS satellites. These low-precision parameters are used by the GPS receiver to estimate the rough position of the GPS satellites and to reduce the searching space for the GPS satellite transmission frequencies[1] and obtaining the precise ephemeris data. Ionospheric model and UTC time calculation parameters are required by the GPS receiver to refine the calculation of delays through the ionosphere [8]. The reason why there are 25 frames is because of the last two subframes, four and five. Subframes four and five have data which cycle through the 25 frames, i.e. almanac data are transmitted for all the 32 GPS satellites[2] in case the receiver found only one satellite and once it collected all almanac data, it can search for other visible GPS satellites. These 25 frames create a masterframe. Once the 25 frames have been transmitted, the process is repeated again.

The data are modulated using the binary phase shift keying (BPSK) technique. The newly modulated signal is the *L1* signal and it is emitted from the satellite directed antennas towards Earth [1]. The BPSK technique works by changing the phase of the carrier signal for 180° at the moment of bit toggle (flipping) in the data [1] [8]. Basic principle of this technique can be seen in figure 2.4. The carrier wave for GPS BPSK modulation is centered at a frequency of 1575.42 MHz [8]. These signals travel an average distance of 20200 km from the satellite to the GPS receiver and are affected by various sources of noise. BPSK modulation is mostly used for satellite links because of its simplicity and immunity to noise and signal intereference for the price of transfering data at low speed rates [14, Chapter 1]. The demodulation process of L1 will be discussed and analysed seperately in section 2.2.1.

[1] Although all satellites transmit on the same one frequency, when the signals are received on Earth, they have a different frequency from the transmitted one. This will be further explained in more details in the following sections 2.2.1, 2.2.2 and 2.2.3.

[2] 24 satellites are used in the GPS system, the rest is used in case one of the 24 fails.

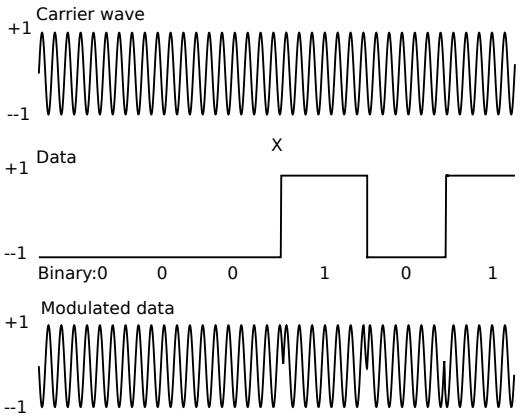

Figure 2.4.: BPSK Modulation - First signal is the carrier wave, and it is multiplied (mixed) with the second signal, which are the data to be transmitted. The resulting signal at the output of the satellite antenna is the third one.

However, before the raw navigation data enter the BPSK modulation process, they are XORed with pseudo random noise (PRN) sequences for different satellites (each satellite owns a unique PRN sequence) [8]. PRN sequences are used to identify which satellite signal is being decoded, transmission of the data on the same frequency as well as to enable the distance measuring mechanism between the satellite and the GPS receiver. Equivalent PRN sequence is generated on the GPS receiver and it is compared with the received PRN sequence which is delayed (shifted) due to the distance. This delay multiplied with the speed of light yields the distance between the satellite and the GPS receiver. PRN sequences have similar autocorrelation properties as noise, when it is shifted in time domain it has a low correlation value whereas when it is matched with exact image of itself it produces a high correlation peak [6, Chapter 3]. This property is used for identifying the satellites and for finding the exact phase shift. The second important property of PRN sequences is the property of orthogonality. This proberty enables the reception of different data on the same frequency, also known as code division multiple access (CDMA). It is important to note that the PRN sequences must have a higher frequency than the data, i.e. the bit duration of a PRN sequence is much shorter than of the data [6, Chapter 3]. Single bits in PRN sequences are called *chips* and the complete sequence as *code* [6, Chapter 3]. This newly generated signal is called direct sequence spread spectrum (DSSS) [6, Chapter 3]. In GPS terminology it is named as Code/Acquisition (C/A) code. C/A code is feed into the BPSK modulation process, where it is mixed with the carrier wave and producing the L1 signal. More details will be given in the C/A demodulation section 2.2.2. Transmission speed of the navigation message is 50 bps, therefore the reception of a complete masterframe requires around $\approx$ 12.5 minutes,

i.e. $(1500\,\text{bitsperframe} \cdot 25\,\text{frames})/(50\,\text{bps} \cdot 60\,\text{s})$.

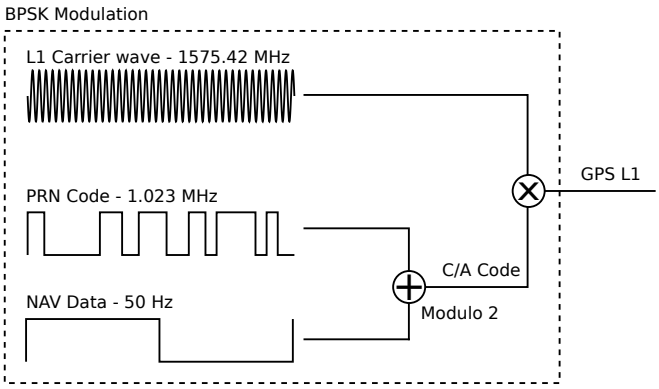

Figure 2.5.: Modulation of the GPS signal L1

The described GPS navigation data modulation can be seen in figure 2.5 and it can be represented in form of equation (2.1) [20], where $D(t)$ are the navigation data at the moment t, $C(t)$ is the PRN chip at the moment t, $cos(2\pi f_c + \varphi_{SV})$ is the generated carrier wave with frequency f_c and phase φ_{GPS}, P is output power of the transmitter amplifier.

$$S(t) = PD(t)C(t)cos(2\pi f_c + \varphi_{GPS}) \tag{2.1}$$

The equation 2.1 will be rewritten as given in 2.2. It represents the same equation but at the GPS receiver after traveling $\approx 20200\,km$, where $d_{C/A}$ is the C/A data and $n(t)$ is the random noise at moment t influenced by various factors that influence electromagnetic waves.

$$S(t) = \sqrt{\frac{P}{2}} d_{C/A} cos(2\pi f_c + \varphi_{GPS}) + n(t) \tag{2.2}$$

The GPS satellites are positioned in orbits so that at every moment at any spot on Earth, at least four satellites are visible (a spot can be considered as a mountain peak since in the cities GPS signals are blocked by buildings). In the next section, more details will be revealed on the process of demodulating the GPS L1 signal and acquiring the correct time and position.

2.2. GPS signal acquisition and demodulation

GPS satellites[3] orbiting our planet, at a distance of approximately $20200\,km$, are equiped with precise atomic clocks [12, Chapter 2.7]. These atomic clocks are calibrated and maintained on a daily basis by the U.S. Air Force [18]. The time the atomic clock generate, refered earlier as GPS system time, denoted as t_{SV}, is generated as a time stamp at the moment of the subframe broadcast [2]. In addition to the broadcast time, subframe 1 contains parameters to account for the deterministic clock errors embedded in the broadcasted GPS system time stamp. These errors can be characterized as bias, drift and aging errors [2]. The correct broadcast time, denoted as t, can be estimated using the model given in equation (2.3) [2]. In equation (2.4), where the GPS receiver is required to calculate the satellite clock offset, denoted as Δt_{SV}, a number of unknown terms can be seen. These terms are encapsulated inside of the transmitted frames. The polynomial coefficients: a_{f0} - *clock offset*, a_{f1} - *fractional frequency offset*, a_{f2} - *fractional frequency drift*; and t_{0c} - *reference epoch* are encapsulated inside of subframe 1. The only remaining unknown term left in equation (2.4) is the *relativistic correction term*, denoted as Δt_r. Δt_r can be evaluated by applying the equation given in (2.5). F is a constant calculated from the given parameters in (C.0.7) and (C.0.8), whereas e, $\sqrt{A}$ and E_k are orbit parameters encapsulated in subframes 2 and 3 [2].

$$t = t_{SV} - \Delta t_{SV} \tag{2.3}$$

$$\Delta t_{SV} = a_{f0} + a_{f1}(t_{SV} - t_{oc}) + a_{f2}(t_{SV} - t_{oc})^2 + \Delta t_r \tag{2.4}$$

$$\Delta t_r = F e \sqrt{A} \sin E_k \tag{2.5}$$

$$F = \frac{-2\sqrt{\mu_e}}{c^2} = -4.442807633 \cdot 10^{-10} \frac{s}{\sqrt{m}} \tag{2.6}$$

Nevertheless, the broadcast satellite time information is not sufficient to estimate the precise time at the moment of the signal arival. Even though the signal arrives in approximately[4] $77\,ms$, the precision of the atomic clock is in the range of 10 ns [12, Chapter 2]. Undoubtedly the signal propagation (travel) time, denoted as t_{prop}, has to be taken into account. In that case, the exact time at the moment of arival is known, denoted as t_{exact} and is given in equation (2.7). Propagation time is computed by measuring the phase shift of the C/A signal, more details will be given in sections

[3] Ssatellites are named as space vehicles in GPS terminology and the abrevation SV is used in the equation notations to denote a parameter related to the satellite itself.

[4] Propagation time depends on user and GPS satellite position.

2.2.2 and 2.3. More importantly, t_{exact} time will be later used to synchronize various time dependent systems like the GSM, LTE, GNSS or other communication and ranging systems.

$$t_{exact} = t_{prop} + t \tag{2.7}$$

2.2.1. Carrier wave demodulation

In order to calculate the signal propagation time between the satellite and the receiver, the internal sine wave synthesizer inside of the receiver has to be synchronized with the carrier sine wave generator of the GPS satellite [35]. In other words, the identical carrier wave replica has to be generated on the receiver as on the satellite [9]. However, the received signal is not the equivalent of the transmitted signal. Due to the nature of the Doppler effect[5] and wave propagation, the transmitted signal arrives phase disordered at the receiver [35]. This phase disorder is a consequence of the relationship between the instantaneous frequency and instantaneous phase according to equations (2.8) and (2.9).

$$f(t) = \frac{1}{2\pi}\frac{\partial}{\partial t}\phi(t) \tag{2.8}$$

$$\phi(t) = 2\pi \int_{-\infty}^{t} f(\tau)d\tau \tag{2.9}$$

Considering that the GPS satellites orbit the Earth with a speed of around $3.9\,km/s$, the Earth rotates around its axis and the target user with the GPS receiver may move as well, the Doppler effect is unavoidable. The observed phase at the receiver antenna, denoted as φ_o, can be described using the equation given in (2.10), where φ_{GPS} represents the known satellite carrier wave phase, $\delta\varphi_{SV}$ the clock instabilities on the GPS satellite, φ_a the phase shift error caused by propagation delays in the ionosphere and troposphere respectively, $\delta\varphi_{DE}$ the phase shift caused by the Doppler effect and $\delta\varphi_w$ is the wideband noise phase shift.

$$\varphi_o = \varphi_{GPS} + \delta\varphi_{SV} + \varphi_a + \delta\varphi_{DE} + \delta\varphi_w \tag{2.10}$$

The task of the demodulation process is to generate a replica carrier wave with the matching phase shift and mix it with the incoming signal. In the ideal case the

[5] Doppler effect is a phenomenon that happens as a result of relative motion of the two bodies, transmitter and receiver, towards or away from each other and causes frequency shift of the electromagnetic wave [41, Chapter 4].

observed phase on the antenna and the generated phase on the receiver, denoted as φ_{rec}, cancel each other out, that is to say, equation (2.11) equals zero.

$$\Delta\varphi = \varphi_o - \varphi_{rec} \tag{2.11}$$

The circuit responsible for generating the same carrier wave is the phase locked loop (PLL). The PLL circuit is a feedback loop that modifies the synthesized wave parameters such that $\Delta\varphi \approx 0$, a phase shift is shown in figure 2.6.

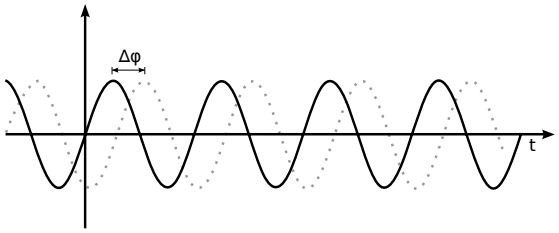

Figure 2.6.: Two equivalent carrier waves with the same frequency but different phase shift

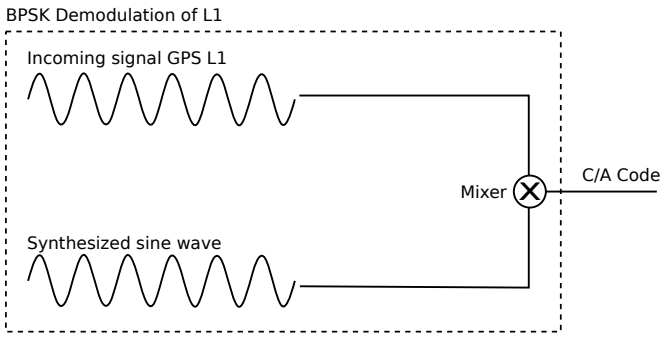

Figure 2.7.: Demodulation of the L1 GPS signal

The reason for this is straightforward to understand by looking at the multiplication of two sine waves. The GPS L1 signal demodulator at the receiver is depicted in figure 2.7, the incoming signal L1 is multiplied with the synthesized sine wave (multiplication is the function of a mixer, denoted as $\otimes$ in figure 2.7). For the purpose of easier analysis, cosine waves will be used istead of sine waves, the difference between them is only in the phase shift, as denoted in equation (2.12).

$$\sin(\pm x) = \cos\left(\frac{\pi}{2} \pm x\right) \tag{2.12}$$

Multiplication of two cosine waves, as in equation (2.13), can be derived by adding $\cos(A+B)$ and $\cos(A-B)$ together, as respectively given in equations (2.14) and (2.15).

$$\cos(A)\cdot\cos(B) = \frac{1}{2}\cos(A-B) + \frac{1}{2}\cos(A+B) \tag{2.13}$$

$$\cos(A+B) = \cos(A)\cos(B) - \sin(A)\sin(B) \tag{2.14}$$

$$\cos(A-B) = \cos(A)\cos(B) + \sin(A)\sin(B) \tag{2.15}$$

The incoming GPS L1 signal with a frequency f_1, given in figure 2.7, can be written as $d_{C/A}\cos(\omega_1 t)$, a similar form is given in equation (2.2), where $\omega_1 = 2\pi f_1$ is the angle frequency and $d_{C/A}$ is the C/A data (navigation message modulated with the PRN code), $d_{C/A} = d_{PRN} \oplus d_{NAV}$. If equation (2.13) is rewritten with the received GPS signal L1 and synthesized wave with frequency f_2, the equation results the one given in (2.16)

$$d_{C/A}\cdot\cos(\omega_1 t)\cos(\omega_2 t) = \frac{1}{2}d_{C/A}\cdot\cos(\omega_1 t-\omega_2 t) + \frac{1}{2}d_{C/A}\cos(\omega_1 t+\omega_2 t) \tag{2.16}$$

This leaves the resulting signal with two frequency terms, a low frequency term $(\omega_1 t-\omega_2 t)$ and a high frequency term $(\omega_1 t+\omega_2 t)$, the t can be taken in front of the bracket as it is a common multiplier. The high frequency term, $(\omega_1+\omega_2)$, can be filtered out using a low-pass filter[6]. Ideally, the difference of the angle frequencies is zero, as in equation (2.17), since $\cos(\Delta\omega) = \cos(0) = 1$ and the remaining left signal is only the C/A code multiplied with the DC term (zero frequency producing a constant voltage) leaving only $\frac{1}{2}d_{C/A}$.

$$\Delta\omega = \omega_1 - \omega_2 = 0 \tag{2.17}$$

However, if the frequencies do not match, $f_1 \neq f_2$, then the output signal $\frac{1}{2}d_{C/A}$ will be modified by the residual frequency $f_1 - f_2$, and subsequently this will change the demodulated C/A output (also known as phase shift). Under those circumstances the correlator will be unable to match the C/A code with the correct PRN code. An illustration of this phenomenon is depicted in figure 2.8.

[6] A low-pass filter passes low frequency signals and attenuates high frequency signals. In other words, signals higher than the specified cutoff frequency of the low-pass filter, are cut off by reducing their amplitudes.

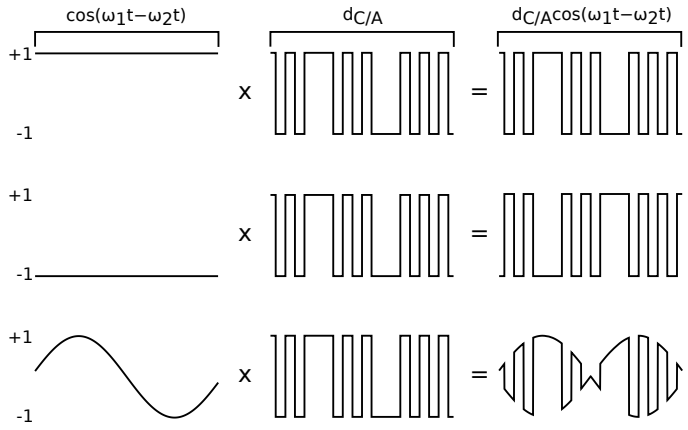

Figure 2.8.: Effects of the low frequency term on the demodulated output C/A wave on the GPS receiver (the explanations and figures are from top to bottom). If the synthesized frequency is correct, $f_1 = f_2$, the low frequency term becomes a DC term and does not modify the output $d_{C/A}$ wave (first figure). If the frequency matches but the phase not, in this case the phase is shifted for π, then $d_{C/A}$ is inverted (second figure). If the phase shifts with time, then the amplitude and phase of $d_{C/A}$ will vary as well (third figure).

2.2.2. C/A wave demodulation

As a result of the previous step, one can continue with the demodulation of the C/A wave. Demodulating the C/A wave with the PRN code will result in the time and navigation data. Each tracked GPS satellite signal is demodulated seperately using the same PRN code, code chipping rate and carrier frequency-phase (which was determined above) for the given satellite [15, Chapter 4]. The PRN codes for each GPS satellite is well defined and known by the GPS receiver. The receiver has to generate the equivalent PRN code with matching code chipping rate (phase) of the transmitted C/A code, this is depicted in figure 2.9 [15, Chapter 5]. This phase shift is again a consequence of the Doppler effect described in section 2.2.1. For the particular example, the matching phase shift was achieved with the second replica PRN code, with a phase shift of $\tau = 0$ but there could be a case with any other value of τ, $\tau \in [0, 1022]$. Implementation of the PRN code synthesizer depends on the GPS receiver manufacturer but it is usually implemented as a linear feedback shift registers (LFSR) that produces an output according to a predefined function $f(\tau)$. This function, $f(\tau)$, generates an PRN code, that is delayed in phase by τ, where τ is a multiple of the chipping rate period $T_c = 977.5\,ns$. The chipping period T_c can be derived from equation (2.18). The amount of time required to find a matching

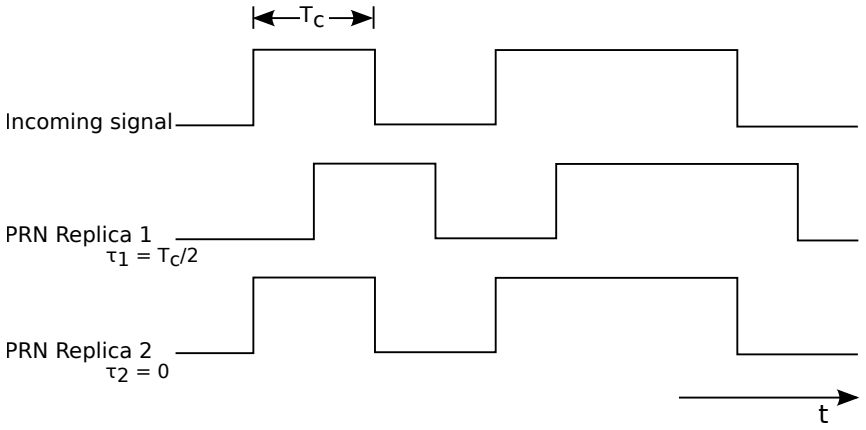

Figure 2.9.: Comparison between the original C/A code generated on the GPS satellite with two synthesized PRN codes with a different phase shift on the receiver.

PRN code shift, τ, on the receiverr is proportional to the amount of parallely working LFSRs on the system [6, Chapter 3]. Clearly with more LFSRs the required time for finding the matching phase shift increases.

$$T_c = \frac{1}{f_{PRN}} = \frac{1}{1.023 \cdot 10^6 \text{Hz}} \tag{2.18}$$

To determine whether the synthesized PRN code, matches the incoming C/A code of the received satellite signal, known correlation properties of PRN codes are used, as described in section 2.1. Since the PRN code is modeled as a sequence of +1's and -1's, the autocorrelation of a signal is at its maximum if it is in phase, i.e. summing up the sequence products yields the absolute maximum value for the case where each bit from one signal matches the bit from the other signal. As an illustration of the idea, an example is given in figure 2.10. The cross-correlation of the incoming C/A code with the first synthesized PRN code produces a result of $-3 = (+1) \cdot (-1) + (-1) \cdot (+1) + (+1) \cdot (-1) + (+1) \cdot (+1) + (-1) \cdot (+1)$, whereas the cross-correlation of the incoming C/A code and the second synthesized PRN code yields a result of $+5 = (+1) \cdot (+1) + (-1) \cdot (-1) + (+1) \cdot (+1) + (+1) \cdot (+1) + (-1) \cdot (-1)$.

The same principle applies to the transmitted C/A and generated PRN code sequences in the GPS receiver. Thus, this can be modeled using the equation given in (2.19), where $G_i(t)$ is the C/A code[7] as a function of time t, for the GPS satellite i; $T_{C/A}$ is the C/A chipping period of $977.5\,ns$ and τ is the phase shift in the auto-correlation function [15, Chapter 4].

[7] PRN generated code for GPS satellites is called Gold code sequences since they were first discovered by Dr. Robert Gold.

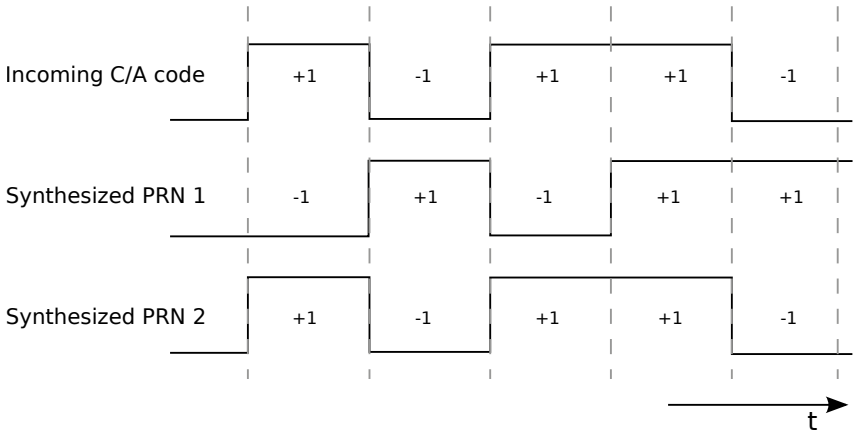

Figure 2.10.: Cross-correlation on three different signals

$$R_i(t) = \frac{1}{1023 \cdot T_{C/A}} \int_{t=0}^{1022} G_i(t) G_i(t+\tau) d\tau \tag{2.19}$$

Another correlation property of the PRN codes is used, the fact that in the ideal case the cross-correlation of two different PRN codes yields a result of zero. The ideal case of PRN code can be modeled as in equation (2.20),

$$R_{ij}(\tau) = \int_{-\infty}^{+\infty} PRN_i(t) PRN_j(t+\tau) d\tau = 0 \tag{2.20}$$

where PRN_i is the PRN code waveform for GPS satellite i and PRN_j is the PRN code waveform for every other GPS satellite other than i, $i \neq j$ [15, Chapter 4]. Equation (2.20) "states that the PRN waveform of satellite i does not correlate with PRN waveform of any other satellite j for any phase shift τ" [15, Chapter 4]. Without the property given in (2.20), the GPS receiver would not be able to smoothly differentiate between different GPS satellite signals. Once the phase shift, τ, has been found, the C/A code is modulated (XORed) with it. The resulting binary code will be the navigation message. The implementation problem of finding correct C/A and carrier wave demodulation will be further explained in the following section 2.2.3.

2.2.3. Implementation of the 2D search space problem

In the following paragraphs an introduction will be given on the implementation problems of the previously mentioned concepts. As it can be seen, from subsections 2.2.1 and 2.2.2, decoding the GPS navigation message is a 2D search space problem for each GPS satellite signal acquisition. The 2D search space is limited by well

known physical properties of the GNSS system such as the motion speed of GPS satellites (and the receiver) as well as the frequency oscillator on the receiver.

GPS satellites move toward or away from the GPS receiver with a speed of 800 m/s [12, Chapter 3]. The Doppler effect on the frequency of the satellite can be estimated using equation (2.21), where f_e is the emitting frequency (L1), v_{SV} is the speed of the satellite towards (away from) the receiver and c is the speed of light.

$$f_{DE} = f_e \frac{v_{SV}}{c} \tag{2.21}$$

By inserting the appropriate values in equation (2.21) yields a result of ≈ 4.2 kHz, for 800 m/s and ≈ −4.2 kHz (if the satellite moves away from the GPS receiver then the speed is taken as negative). This makes a total range of ≈ 8.4 kHz. The Doppler effect of the GPS receiver motion can be ignored since for each 1 km/h of movement, it affects the frequency range for ≈ 1.46 Hz.

On the other hand, the frequency offset induced by the reference oscillator in the GPS receiver can not be ignored. Function of the reference oscillator is to give the GPS receiver the clock pulse required for all the computations and comparisons. The frequency search space is "additionaly affected for 1.575 kHz of unknown frequency offset for each 1 ppm (*parts per million*) of the unknown receiver oscillator offset" [12, Chapter 3]. The reference oscillators in GPS receivers have typically an offset of $\pm 0.5, \pm 1, \pm 2, \pm 3,$ or $\pm\, 5$ ppm [11], [12, Chapter 3], the standard in smart phone design has been set to ±2.5 ppm [34]. In the worst case this makes the unknown frequency to be in range of 10 kHz – 25 kHz.

A typical receiver searches in frequency bands (bins) of several hundred Hz [20]. Commonly used frequency bin size is 500 Hz, therefore there are about 20-50 bins to search (10000 Hz/500 Hz = 20) [12, Chapter 3]. The frequency search bin (band) size is a function of the desired peak magnitude loss (signal to noise ratio) due to the frequency mismatch and integration time period. Larger frequency bands mean a smaller number of bins to search but a greater correlation peak magnitude loss, i.e. with larger frequency bands it gets harder to identify the correlation peaks described in sections 2.1 and 2.2.2. The frequency search bin size can be estimated using the frequency mimsmatch loss *sinc* function given in equation (2.22) [30], [12, Chapter 6], where Δf is the frequency mismatch in Hz, in other words it represents the difference between the received signal frequency and the synthesized carrier frequency on the receiver; and T_{ci} is the coherent integration time (usually $0.5\,ms$ according to [30] and [12, Chapter 3] but depends on the implementation).

$$D_F = \left| \frac{\sin(\pi \Delta f T_{ci})}{\pi \Delta f T_{ci}} \right| \tag{2.22}$$

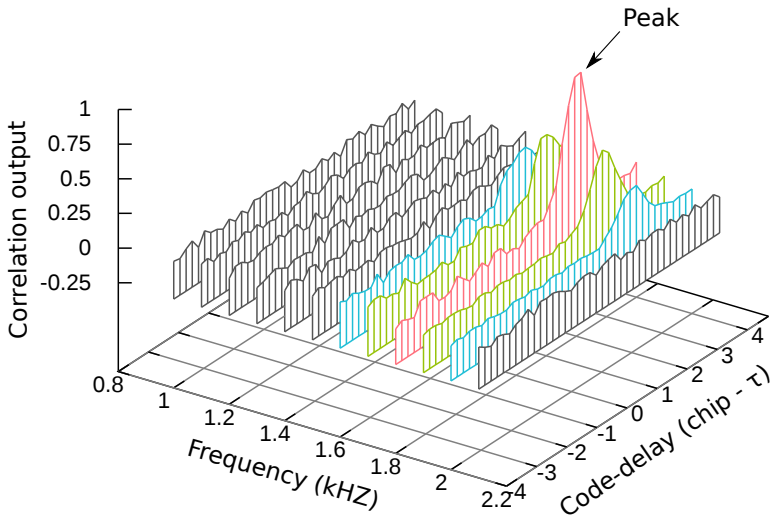

Figure 2.11.: Segment of the frequency/code delay search space for a single GPS satellite

The frequency mimsmatch loss sinc function, D_F, is evaluated in dB, therefore for a loss of $\approx 0.98\,\text{dB}$, the frequency mismatch ought to be $\Delta f = 250\,\text{Hz}$, due to the fact that the maximum loss will occur when the frequency is differing by 1/2 of the bin spacing. That is to say, for a bin space of 500 Hz, it is 250 Hz.

"The total range of possible GPS code delays is $1\,ms$. This is because the GPS C/A PRN code is $1\,ms$ long, and then it repeats. The PRN code chipping rate is 1.023 MHz, and there are 1023 chips in the complete $1\,ms$ epoch" [12, Chapter 3].

For the purpose of better understanding, a segment of the frequency/code delay search space is shown in figure 2.11. The peak implies the correct frequency and code delay have been found. In figure 2.11 smaller frequency bins have been used so that the concept becomes understandable to the reader.

The speed of searching the 2D search space (finding the peak) depends on the complexity and strategy of the implemented algorithm [8, Chapter 6]. In the worst case, there are in total 102300 conbinations in the search space, this can be derived from equation (2.23), visually shown in figure 2.12.

$$\text{Search Space} = 50\,(\text{bins}) \cdot 1023\,(\text{C/A codes}) \cdot 2\,(\text{Phases per C/A chip}) \tag{2.23}$$

The common strategy is to start searching from the middle frequency bins and to jump up and down until the entire search space has been exhausted (first 500 Hz, second -500 Hz, then in the 1000 Hz bin and then in the -1000 Hz bin), as shown in

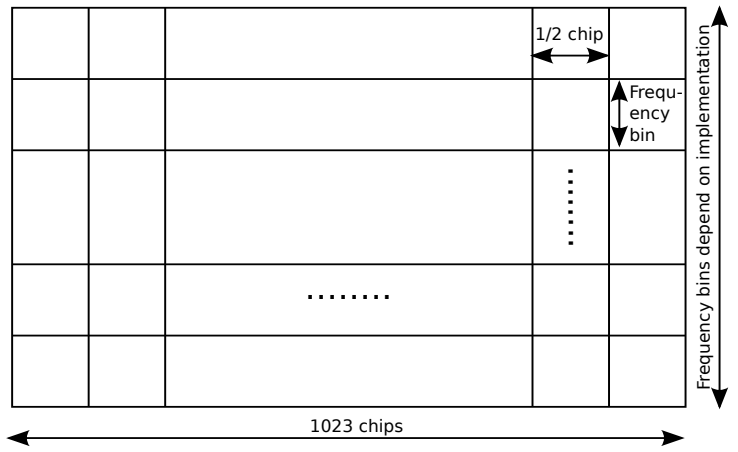

Figure 2.12.: The total search space

figure 2.13 [12, Chapter 3]. This procedure is performed when no extra information are known by the receiver (almanac data are missing), i.e. first time the GPS receiver is turned on. It is known under the name of cold start.

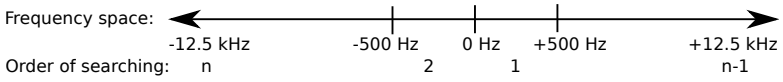

Figure 2.13.: Idea of the frequency searching algorithm

There are three different working modes when it comes to searching for the GPS satellites. If no information are known, when some information are known and when almost all information are known. These three modes are known as *cold* (as mentioned earlier), *warm* and *hot* start. They differ from each other by the amount of known information by the GPS receiver. Cold start indicates the GPS receiver has no almanac, ephemeris, oscillator offset and time data. In order to track the satellites faster next time the GPS receiver is started, it stores the previously mentioned data (last known almanac, ephemeris, oscillator offset, time and position data) in its electrically erasable programmable read only memory (EEPROM). This new type of start, is known as a warm start, provided that the data in the receivers' EEPROM are not older than 180 days and its real time clock counter was constantly updated. In this case, the receiver uses the previously saved information to estimate the position of the satellites, therefore the Doppler effects can be roughly estimated. As a consequence of the known Doppler effect, the frequency bin where to start the search first is known this time [12, Chapter 3]. Hot start works the same way, only the ephemeris data and time data are precisely known (time ought to be known in accuracy of submilliseconds).

2.3. Distance and position estimation

In this section the focus is set on distance and position estimation inside of the GPS receiver. GPS system, as mentioned earlier, takes advantage of the TOA ranging concept to determine user position. Time is measured how long it takes for a signal to arrive from a known location. In figure 2.14, an example concept can be seen,

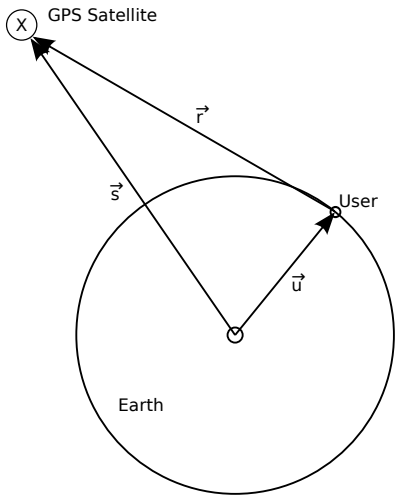

Figure 2.14.: Basic distance estimation principle for one satellite

where $\vec{u} = (x_u, y_u, z_u)$ represents the unknown GPS user position vector with respect to Earth-Centered, Earth-Fixed[8] (ECEF) coordinate system, $\vec{r}$ is the distance vector from the satellite to the user and $\vec{s} = (x_s, y_s, z_s)$ represents the GPS satellite position with respect to ECEF at a timepoint. Vector $\vec{s}$ is computed from ephemeris data broadcasted by the satellite. The distance vector $\vec{r}$, distance between the satellite and user, can be computed using equation (2.24) and its magnitude is given in equation (2.25).

$$\vec{r} = \vec{s} - \vec{u} \tag{2.24}$$

$$r = \|s - u\| \tag{2.25}$$

The geometric distance of r is computed by measuring the signal propagation time, this is illustrated in figure 2.15 and it was mentioned in section 2.2.2. The PRN code generated on the GPS satellite at time t_1 arrives at the time t_2, the difference between these two time stamps, Δt, represents the propagation time. By multiplying the propagation time, Δt, with the speed of light, c, the geometric distance r is computed, as given in equation (2.26).

[8] ECEF is a Cartesian coordinate system where the point $(0, 0, 0)$ is defined as the center of mass of the Earth [10].

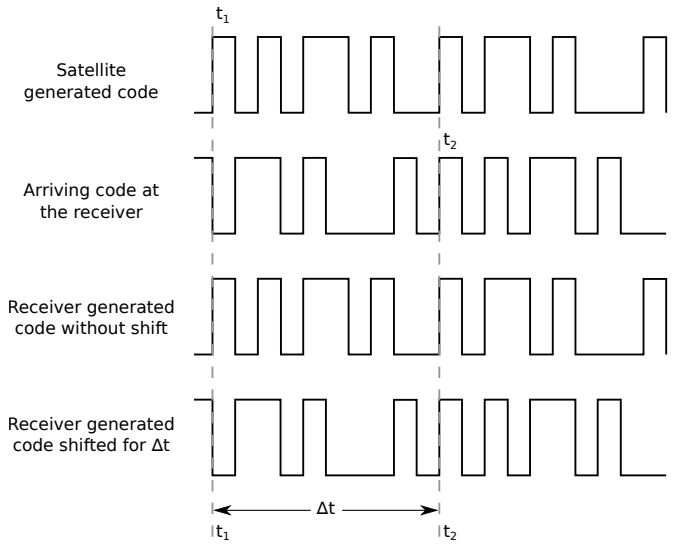

Figure 2.15.: Estimating the distance by phase shift $\Delta t = t_2 - t_1 = \tau$

$$r = c\Delta t \tag{2.26}$$

Since the clocks are not synchronized, as described in sections 2.2 and 2.2.3, clock error offsets have to be added to the geometric distance r. This new distance is called *pseudorange*, ρ, because the range is determined using the difference of two nonsynchronized clocks (one on the GPS satellite and the other one on the receiver) that generate PRN codes[9]. Pseudorange is calculated as given in equation (2.27), where t_u is the advance of the receiver clock with respect to the system time[10] and δt is the offset of the satellite clock from the system time [15].

$$\rho = r + c(t_u - \delta t) \tag{2.27}$$

Equation (2.25) can be rewritten as (2.28) with respect to equation (2.27).

$$\rho - c(t_u - \delta t) = \|s - u\| \tag{2.28}$$

Offset of the satellite clock from the system time, δt, is updated from Earth, as mentioned in 2.2 and for that reason it can be removed for sake of simplicity, i.e. it is not an unknown term anymore, then the eqaution (2.28) can be rewritten as (2.29).

$$\rho - ct_u = \|s - u\| \tag{2.29}$$

In order to estimate the user (GPS receiver) position, advance of the receiver clock with respect to the system time, t_u, has to be found, in other words equation (2.30)

[9] pseudo - Not genuine; sham; not perfect.
[10] System time is the exact time on Earth and it is the most precise time known!

has to be solved, where i is the index of visible satellites at the moment of signal reception [15].

$$\rho_i = \|s_i - u\| + ct_u \tag{2.30}$$

The estimated position of the user, $\vec{u} = (x_u, y_u, z_u)$, is a three dimensional vector and as mentioned above the clock offset, t_u, is unknown as well. This four dimensional space requires to have at least four pseudorange equations (2.30) to find all the four unknown terms. As a result of this fact, at least four satellites have to be visible at the same time to estimate the position of the target user. Equation given in (2.30) takes the form in (2.31) because the coordinate system is Cartesian and ρ_i is nothing else but Euclidean distance where $i = 1, 2, ..., n$ such that $n \geq 4$ and $\vec{s_i} = (x_i, y_i, z_i)$ is the satellite position estimated from the ephemeris data.

$$\rho_i = \sqrt{(x_i - x_u)^2 + (y_i - y_u)^2 + (z_i - z_u)^2} + ct_u \tag{2.31}$$

Undoubtedly, the given equation in (2.31) is a nonlinear equation[11]. It is not straightforward to find explicit solutions of nonlinear equations, it is more difficult than compared to linear equations. There are different techniques to solve sets of nonlinear equations [15, Chapter 7] but in this work the linearization method[12] will be presented to find the unknown terms (x_u, y_u, z_u, t_u), i.e. out of an approximate position and clock offset the true user position and the true clock offset will be calculated.

$$\rho_i = \sqrt{(x_i - x_u)^2 + (y_i - y_u)^2 + (z_i - z_u)^2} + ct_u = f(x_u, y_u, z_u, t_u) \tag{2.32}$$

Let the equation (2.31) for pseudoranges, be rewritten as a function f of four unknown terms x_u, y_u, z_u and t_u, as given in (2.32) [15, Chapter 2]. Suppose that the approximation of the position and the clock offset are known, denoted as $\hat{x_u}$, $\hat{y_u}$, $\hat{z_u}$ and $\hat{t_u}$, then equation (2.32) can be rewritten as an approximate pseudorange (2.33).

$$\hat{\rho_i} = \sqrt{(x_i - \hat{x_u})^2 + (y_i - \hat{y_u})^2 + (z_i - \hat{z_u})^2} + c\hat{t_u} = f(\hat{x_u}, \hat{y_u}, \hat{z_u}, \hat{t_u}) \tag{2.33}$$

In other words, the unknown true position terms x_u, y_u, z_u and the clock offset term t_u, of the GPS receiver, will be expressed by the approximate values and an incremental component as shown in equation (2.34) [15].

$$\begin{aligned} x_u &= \hat{x_u} + \Delta x_u \\ y_u &= \hat{y_u} + \Delta y_u \\ z_u &= \hat{z_u} + \Delta z_u \\ t_u &= \hat{t_u} + \Delta t_u \end{aligned} \tag{2.34}$$

[11] Nonlinear equations, also known as polynomial equations, are equations that cannot satisfy both of the linearity properties: additivity $f(x + y) = f(x) + f(y)$ and homogeneity $f(\alpha x) = \alpha f(x)$, $\alpha \in \mathbb{R}$ [32].

[12] Linear approximation is a technique where a function is approximated using a linear function.

By inserting the terms from (2.34) into equation (2.32), a new equation is derived as in (2.35).

$$f(x_u, y_u, z_u, t_u) = f(\hat{x_u} + \Delta x_u, \hat{y_u} + \Delta y_u, \hat{z_u} + \Delta z, \hat{t_u} + \Delta t_u) \tag{2.35}$$

In the next step the pseudorange function will be approximated using Taylor series[13] (linearization of the nonlinear equation). Taylor series for a function $f(x)$ is given in equation (2.36), where as a approches x the estimation error will be smaller and smaller, i.e. $f(x) = f(a)$ when $x = a$. The approximation error depends on Taylor polynomial degree (the amount of terms or taken derivatives of the function) and how far away the point a is from x [38, Chapter 11.9]. The basic idea of the principle can be seen in figure 2.16.

$$f(x) = \sum_{n=0}^{\infty} \frac{f^{(n)}(a)}{n!}(x-a)^n = f(a) + \frac{f'(a)}{1!}(x-a) + \frac{f''(a)}{2!}(x-a)^2 + \ldots \tag{2.36}$$

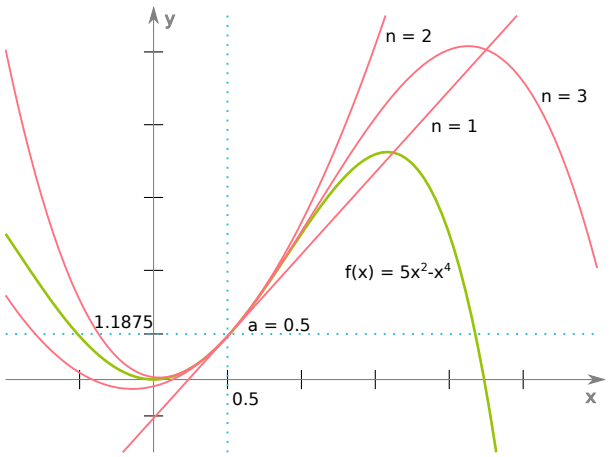

Figure 2.16.: Taylor series approximation for a point $a = 0.5$ where n is the Taylor polynomial degree.

Due to the four unknown terms, Taylor series for multivariables have to be used. The general formula is given in equation (2.37), where vector $\mathbf{x} \in \mathbb{R}^n$ denotes n variables, ∇ (nabla) is the Del[14] operator given in (2.38) and $\mathbf{a}$ is the linearization point of interest [23].

$$f(\mathbf{x}) \approx f(\mathbf{a}) + \nabla f|_{\mathbf{x}=\mathbf{a}} \cdot (x-a) \tag{2.37}$$

$$\nabla^T = \left[\frac{\partial}{\partial x_1} \ldots \frac{\partial}{\partial x_n}\right] \tag{2.38}$$

[13] Taylor series "is a representation of a function as an infinite sum of terms that are calculated from the values of the function's derivatives at a single point" [38, Chapter 11].

[14] Del, ∇, is the vector differential operator.

One can note that in equation (2.37) the Taylor series polynomial is of the first degree. This is because of one reason, it linearizes the approximation of the function $f(\mathbf{x})$ at point $\mathbf{a}$ and as a consequence it removes the nonlinearities [15] [38, Chapter 11.10], as seen in figure 2.16, for $n = 1$ the resulting function is linear. In the previously described step, one would calculate a hyperplane tangent to a point a in a n-Dimensional space. By inserting equation (2.35) in equation (2.37), it yields equation (2.39) where $\mathbf{x} = (x_u, y_u, z_u, t_u)$ and $\mathbf{a} = (\hat{x_u}, \hat{y_u}, \hat{z_u}, \hat{t_u})$.

$$\begin{aligned} &f(\hat{x_u} + \Delta x_u, \hat{y_u} + \Delta y_u, \hat{z_u} + \Delta z, \hat{t_u} + \Delta t_u) \approx f(\hat{x_u}, \hat{y_u}, \hat{z_u}, \hat{t_u}) \\ &+\frac{\partial f(\hat{x_u}, \hat{y_u}, \hat{z_u}, \hat{t_u})}{\partial \hat{x_u}} \Delta x_u + \frac{\partial f(\hat{x_u}, \hat{y_u}, \hat{z_u}, \hat{t_u})}{\partial \hat{y_u}} \Delta y_u \\ &+\frac{\partial f(\hat{x_u}, \hat{y_u}, \hat{z_u}, \hat{t_u})}{\partial \hat{z_u}} \Delta z_u + \frac{\partial f(\hat{x_u}, \hat{y_u}, \hat{z_u}, \hat{t_u})}{\partial \hat{t_u}} \Delta t_u \end{aligned} \tag{2.39}$$

The terms from equation (2.39) are solved individually in equations (2.40) where $\sqrt{(x_i - \hat{x_u})^2 + (y_i - \hat{y_u})^2 + (z_i - \hat{z_u})^2}$ has been subsituted with $\hat{r_i}$.

$$\begin{aligned} \frac{\partial f(\hat{x_u}, \hat{y_u}, \hat{z_u}, \hat{t_u})}{\partial \hat{x_u}} &= \frac{1}{2} \frac{-2(x_i - \hat{x_u})}{\sqrt{(x_i - \hat{x_u})^2 + (y_i - \hat{y_u})^2 + (z_i - \hat{z_u})^2}} = -\frac{x_i - \hat{x_u}}{\hat{r_i}} \\ \frac{\partial f(\hat{x_u}, \hat{y_u}, \hat{z_u}, \hat{t_u})}{\partial \hat{y_u}} &= \frac{1}{2} \frac{-2(y_i - \hat{y_u})}{\sqrt{(x_i - \hat{x_u})^2 + (y_i - \hat{y_u})^2 + (z_i - \hat{z_u})^2}} = -\frac{y_i - \hat{y_u}}{\hat{r_i}} \\ \frac{\partial f(\hat{x_u}, \hat{y_u}, \hat{z_u}, \hat{t_u})}{\partial \hat{z_u}} &= \frac{1}{2} \frac{-2(z_i - \hat{z_u})}{\sqrt{(x_i - \hat{x_u})^2 + (y_i - \hat{y_u})^2 + (z_i - \hat{z_u})^2}} = -\frac{z_i - \hat{z_u}}{\hat{r_i}} \\ \frac{\partial f(\hat{x_u}, \hat{y_u}, \hat{z_u}, \hat{t_u})}{\partial \hat{t_u}} &= c \end{aligned} \tag{2.40}$$

Then by substituting the equation terms from (2.40), (2.32) and (2.33) into (2.39), the resulting equation is given in (2.41).

$$\rho_i = \hat{\rho}_i - \frac{x_i - \hat{x_u}}{\hat{r_i}} \Delta x_u - \frac{y_i - \hat{y_u}}{\hat{r_i}} \Delta y_u - \frac{z_i - \hat{z_u}}{\hat{r_i}} \Delta z_u + c\Delta t_u \tag{2.41}$$

At this step, by solving equation (2.39), the linearization of the nonlinear equations is completed.

$$\hat{\rho}_i - \rho_i = \frac{x_i - \hat{x_u}}{\hat{r_i}} \Delta x_u + \frac{y_i - \hat{y_u}}{\hat{r_i}} \Delta y_u + \frac{z_i - \hat{z_u}}{\hat{r_i}} \Delta z_u - c\Delta t_u \tag{2.42}$$

$$\Delta\rho = \hat{\rho}_i - \rho_i \tag{2.43}$$

$$\alpha_{xi} = \frac{x_i - \hat{x_u}}{\hat{r_i}} \qquad \alpha_{yi} = \frac{y_i - \hat{y_u}}{\hat{r_i}} \qquad \alpha_{zi} = \frac{z_i - \hat{z_u}}{\hat{r_i}} \tag{2.44}$$

By rearanging the equation (2.41) one derives equation (2.42). And then by substituting the terms in (2.43) and (2.44) into (2.42), the equation resembles the one given in (2.45).

$$\Delta\rho_i = \alpha_{xi}\Delta x_u + \alpha_{yi}\Delta y_u + \alpha_{zi}\Delta z_u - c\Delta t_u \tag{2.45}$$

There are four unknowns, Δx_u, Δy_u, Δz_u and Δt_u, in equation (2.45). By solving this set of linear equations, which will result in finding Δx_u, Δy_u, Δz_u and Δt_u, the GPS receiver position (x_u, y_u, z_u) and clock offset t_u is computed by replacing the same into equations in (2.34). Equation (2.45) can be rewritten for four satellites in the matrix form as in (2.46).

$$\Delta\boldsymbol{\rho} = \boldsymbol{\alpha}\Delta\boldsymbol{x} \tag{2.46}$$

$$\Delta\boldsymbol{\rho} = \begin{bmatrix}\Delta\rho_1\\ \Delta\rho_2\\ \Delta\rho_3\\ \Delta\rho_4\end{bmatrix} \quad \boldsymbol{\alpha} = \begin{bmatrix}\alpha_{x1} & \alpha_{y1} & \alpha_{z1} & 1\\ \alpha_{x2} & \alpha_{y2} & \alpha_{z2} & 1\\ \alpha_{x3} & \alpha_{y3} & \alpha_{z3} & 1\\ \alpha_{x4} & \alpha_{y4} & \alpha_{z4} & 1\end{bmatrix} \quad \Delta\boldsymbol{x} = \begin{bmatrix}\Delta x_u\\ \Delta y_u\\ \Delta z_u\\ -\Delta c t_u\end{bmatrix} \tag{2.47}$$

Finally, by multiplying both left sides[15] of the equation (2.46) with the inverse term of $\boldsymbol{\alpha}$, it yields the result of the unknown terms, as given in equation (2.49).

$$\boldsymbol{\alpha}^{-1}\Delta\boldsymbol{\rho} = \boldsymbol{\alpha}^{-1}\boldsymbol{\alpha}\Delta\boldsymbol{x} \tag{2.48}$$

$$\Delta\boldsymbol{x} = \boldsymbol{\alpha}^{-1}\Delta\boldsymbol{\rho} \tag{2.49}$$

Linearization is repeated in a loop, where in the next round the approximate positions are set to the just derived position values, that is, $\hat{x_u} = x_u$, $\hat{y_u} = y_u$, $\hat{z_u} = z_u$ and $\hat{t_u} = t_u$. This process is repeated until the approximated positions converge to their final values. It is not necessarily required that the initial positions are very accurate and the results are usually obtained by 4-5 itterations [28]. Risks exist that the solutions will still be corrupted but there are different error avoiding mechanisms to solve these problems, like minimizing the error contribution using more than four satellite measurements [28] [15, Chapter 7].

[15] Matrix multiplication is not communitative, $\mathbf{AB} \neq \mathbf{BA}$.

2.4. Assisted GPS in Wireless networks

In the following paragraphs Assisted GPS (A-GPS) will be presented and how it works. A-GPS receivers work on a "similar principle" as warm/hot start on GPS receivers. Instead of loading the recently saved data from the EEPROM, an external transfer medium is used to deliver the same type of information that are known at a warm/hot start [36], [13], [4]. In this work, the external transfer medium is air and the information are transfered using electromagnetic waves. The existing GSM interface was utilised for the purpose of delivering the data to the smart phone with an A-GPS receiver. The basic scenario can be seen in figure 2.17.

The BTS station is connected to the global navigation satellite system (GNSS) server, which is directly connected to the GPS reference station. The GPS reference station delivers the GNSS server exact time stamps, approximate location, satellite health as well as clock corrections, ionospheric and UTC model, almanac and ephemeris data [4].

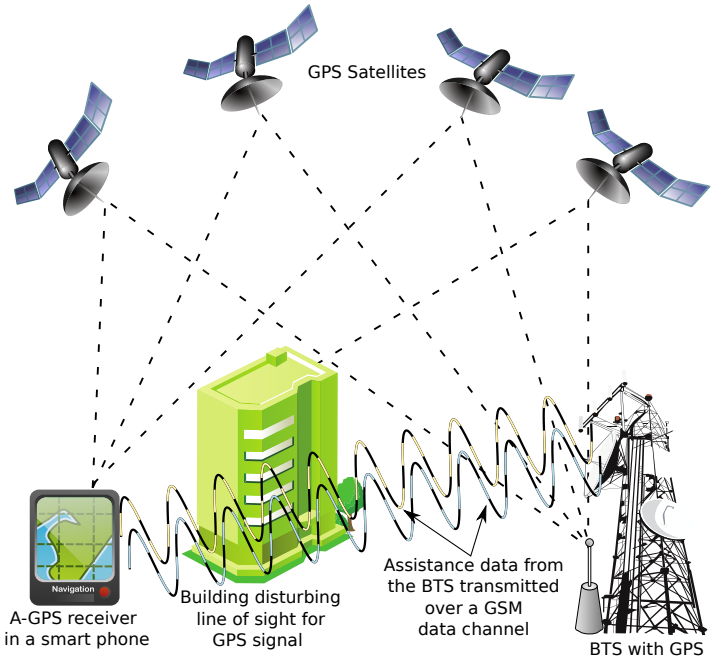

Figure 2.17.: Basic A-GPS principle

Time stamp is not used in GSM networks since it can be off by several seconds and would require additional equipment for synchronizing the network [4], [13]. However in CDMA networks the time stamp is accurate to within $100\,\mu s$ [4]. Approximate

location is typically taken to be the location of the BTS from which the target A-GPS receiver acquires the assistance data. Ephemeris and navigation data obtained by the A-GPS receiver in the smart phone help it to estimate the positions of the GPS satellites. This method can greatly enhance the sensitivity of the receiver especially in urban environments [4].

Conventional GPS receivers require at least up to extra 18 to 30 s to receive and decode the navigation data and to generate a location fix [4]. The bit error rate associated with gathering and decoding data dramatically decreases since the acquired signals can be attenuated by 10 to 20 dB indoors [4] of the nominal −130 dB on a 3 dBi "linearly polarized user receiving antenna[16] (located near ground) at worst normal orientation" [2].

A simplified A-GPS algorithm given in [4] will be presented here. This algorithm benefits in speed the more assistance data is present. As the first satellites are tracked, the A-GPS algorithm has an estimation of the feasible region where the target A-GPS user might be located. Consequently, this feasible region will shrink until the location has been fully estimated [4].

(i) Visible satellites and their positions are identified and computed out of the delivered ephemeris and time data.

(ii) For each visible satellite SV_i, the code phase, τ_i, is estimated.

(iii) Pseudoranges are calculated for each visible satellite SV_i.

(iv) Triangulate the position out of the pseudoranges ρ_i.

Although the A-GPS algorithms can be seen as a set of equations, with more unknowns terms known it is straightforward to solve the set of equations. However, with more of the unknown terms it takes more time to get (decode) them from the satellite messages. One should know various A-GPS algorithms exist, some do not require the exact time component and navigation data to be present in the assistance data [5].

2.5. Error estimation

[16] 3 dBi antenna indicates an antenna with a gain of 3 dB with respect to an isotropic (omnidirectional) antenna [12, Chapter 2].

3. Radio Resource Location Protocol

4. Working

4.1. Zitieren..

citep: [24]
citet: ip.access ltd [24]

5. System

Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet.Test test

Referenz für lorem ipsum

6. Software

Author's test system operated on the ARFCN 877 channel. ARFCN (Absolute Radio Frequency Channel Number) defines the uplink and downlink channel frequency insdide the GSM network [42]. ARFCN 877 corresponds to the uplink frequency of 1,783.2 MHz and a downlink frequency of 1,878.2 MHz, where the uplink direction represents the direction from the nanoBTS to the mobile stations and downlink the opposite direction. The decision to use the ARFCN 877 channel was derived from the fact that the channel was free, measurements were carried out with a spectrum analyser built on the USRP hardware.

6. SOFTWARE

7. Hardware

In the following chapter the author will introduce the reader to the hardware components used in the thesis. The hardware components will be presented according to their importance of building an operational and functional GSM network with GPS localization capabilities. Firstly the nanoBTS will be introduced since it is the main hardware component used for building a basic GSM network infrastructure. Then a short insight into the used GPS receiver will be given. Additionally the mobile stations used for testing of the system will be reviewed. Finally, a hardware connection diagram will be given.

7.1. GSM BTS - nanoBTS

In recent years, there has been an increasing interest in deployment of private cellular networks in remote areas or for research which lead to the devolopment of diverse "low-cost" GSM hardware solutions. According to ip.access[1], the manufacturer of nanoBTS, their hardware product is deployed for coverage of "hard-to-reach places; in-buildings; remote areas; marine and aviation; and public spaces". A nanoBTS with its plastic cover can be seen in Figure 7.1. Our University GSM network consists of three nanoBTS stations. The deployed nanoBTS in author's thesis works in the 1800 MHz frequency range, for which the University of Freiburg had obtained a licence from the Federal Network Agency (German: *Bundesnetzagentur*). The transmission frequencies range between 1805-1880 MHz, with 200 kHz channel spacing and maximal output power of +13 dBm (≈20 mW), whereas the receiving frequencies lie in the range between 1710-1785 MHz and same channel spacing as for transmission of 200 kHz [25].

Check the output powere 20 dBm

Add the Abis over IP protocol

The nanoBTS is equiped with an internal 0 dBi (nominal) omni-directional antenna. However, two external antennas sized 30x36 mm, one for transmission (TX) and the other one for reception (RX) of radio waves were used to extend the coverage area. These antennas are connected via the SMA connectors. By using an RF

[1] http://www.ipaccess.com

Figure 7.1.: nanoBTS with its plastic cover. Image courtesy of ip.access ltd

Check for what NWL is

amplifier and larger antennas, for these frequency ranges, the covered area with the GSM signal reception can be increased. For the gain estimation and radiation angle of the used antennas the measurement equipment was missing and therefore was not conducted and described in this work.

At the bottom of the nanoBTS there are 5 ports, as seen in Figure 7.2. The ports from left to right are: voltage supply, ethernet cable with power supply, USB port, TIB-IN and TIB-OUT. In the next paragraph a brief overview of each port will be given.

The left most port is the power supply port used for supplying the nanoBTS with 48 V DC and is optionally used depending on the cable configuration. In author's hardware configuration the power supply port is not used. The following port is for the ethernet connection with 48 V DC power supply. This port is connected to a power supply that is supplied with the nanoBTS. It extends the ethernet connection with 48 V DC for the normal operation mode of the nanoBTS which is in the range between 38-50 V DC. The power consumtion of the nanoBTS is 13 W. More details on how to interconnect the cables will be given in section 7.3. In the middle of the five port region, the mini USB port can be found. It is used by the manufacturer to write the firmware software to the nanoBTS. The last two ports are the TIB-IN and TIB-OUT port[2]. These two ports are used if the GSM network operator requires more than 11 channels to increase the overall capacity of the network. "Up to 4 nanoBTS can be combined into a multiple TRX cell, increasing the number of supported users per TRX by up to 200%. The TIB-OUT from the Master TRX must be connected to the TIB-IN of the slave TRX. This in turn has its TIB-OUT connected to the next TRX in the chain" [24]. The multiple TRX cell configuration will not be further

[2]TIB stands for Timing Interface Bus

Figure 7.2.: nanoBTS with two external antennas and five connection ports

discussed in this work since the purpose of the work was not to boost the capacity of a GSM network but implementation and testing of the RRLP protocol.

To determine the working state of the nanoBTS, an indicator status LED is located on the left side of the five ports region. After the nanoBTS is connected to the power suplly with the ethernet cable, it will change its color and blink speed according to the state it is in. The states can be seen in the Table given in 7.1 [26].

One of the key limitations of gathering more technical data and the critical aspect of this description lies in the fact, that nanoBTS is not an open source hardware platform and ip.access does not offer more details on their product. The lack of systematic hardware analysis can be seen as a major drawback of working with the nanoBTS hardware. However, the given technical data are sufficient for reproducing and conducting the RRLP tests described in this thesis.

Table 7.1.: Indicator LED status on the nanoBTS

State	Color & Pattern	When	Precedence
Self-test failure	Red - Steady	In boot or application code when a power on self-test fails	1 (High)
Unspecified failure	Red - Steady	On software fatal errors	2
No ethernet	Orange - Slow flash	Ethernet disconnected	3
Factory reset	Red - Fast blink	Dongle detected at start up and the factory defaults have been applied	4
Not configured	Alternating Red/Green - Fast flash	The unit has not been configured	5
Downloading code	Orange - Fast flash	Code download procedure is in progress	6
Establishing XML	Orange - Slow blink	A management link has not yet been established but is needed for the TRX to become operational. Specifically: for a master a Primary OML or Secondary OML is not yet established; for a slave an IML to its master or a Secondary OML is not yet established.	7
Self-test	Orange - Steady	From power on until end of backhaul powe on self-test	8
NWL-test	Green - Fast flash	OML established, NWL test in progress	9
OCXO Calibration	Alternating Green/Orange - Slow blink	The unit is in the fast calibrating state [SYNC]	10
Not transmitting	Green - Slow flash	The radio carrier is not being transmitted	11
Operational	Green - Steady	Default condition if none of the above apply	12 (Low)

7.2. GPS Receiver - NL-402U

In the next paragraphs the used GPS device will be described. In contrast to the earlier described hardware, nanoBTS, which the University of Freiburg already owned, the budget for the GPS receiver was limited and the Navilock NL-402U was bought considering only the single criterion, the price. The Navilock NL-402U GPS receiver is based on the u-blox UBX-G5000 single chipset and is a one chip solution [40]. It can be seen on Figure 7.3 with its passive ceramic patch antenna. 1575,42 MHz is the operating frequency of the receiver which corresponds to the L1 civil frequencies and Coarse/Acquisition (C/A) code. The GPS chipset consists of 50 channels, each channel tracks the transmission from a single satellite [15]. It is important to note, the number of channels inside a GPS receiver interrelates with the amount of time required to get the first fix. Receiver tracking sensitivity is -160 dBm (10^{-16} mW). The GPS receiver communicates with the computer ovet the USB port. Although the GPS receiver uses an USB interface, on the computer it emulates 2 UART ports, which are serial communication interfaces.

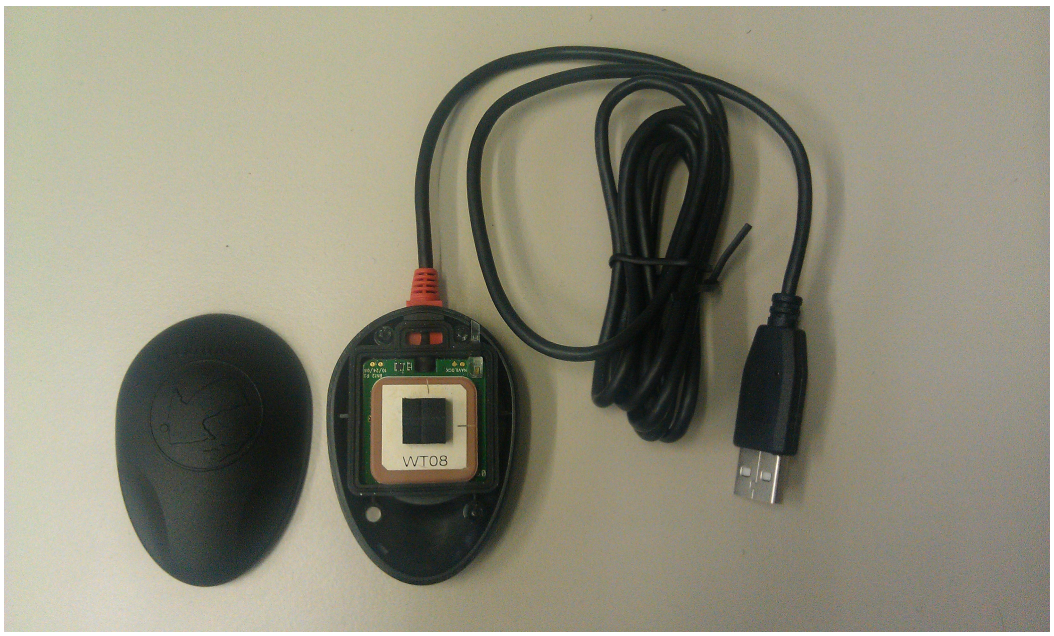

Figure 7.3.: Navilock NL-402U, opened up with the antenna and USB cable

7.3. Cable configuration

In the next section, the author will focus on properly connecting the hardware. At least 4 ethernet cables with RJ45 connectors, on both sides, were required and one switch or hub connected to the internet. One should take notice of the cabling between the nanoBTS and the ethernet switch or hub, since wrong cabling with the power supply unit (PSU) could damage one of the devices. In Figure 7.4, the junction points are label according to the used configuration setting. The ethernet cables between the switch/hub, PSU and nanoBTS should not be longer than 100 m [26].

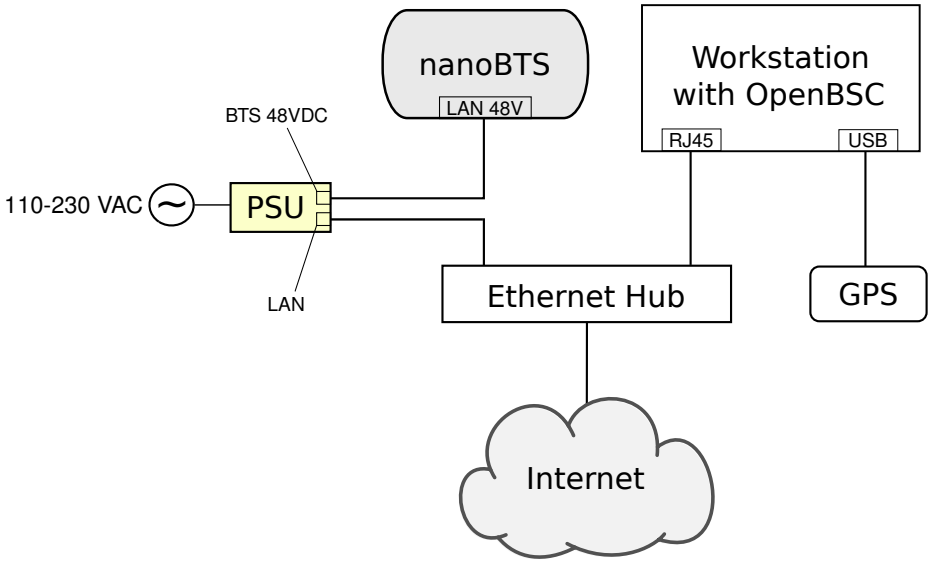

Figure 7.4.: Cable connections, showing interconnection diagram

8. Testing

Test if it can be tricked out by the software Dennis mentioned (protect my privacy)!

8. TESTING

9. Implementation

9. Implementation

10. Future work

10. Future work

11. Summary

11. SUMMARY

Dictionary of acronyms

- *ARFCN* - Absolute Radio Frequency Channel Number - The channel number specifies the physical frequency channel used for transmission and reception of radio waves inside of an BTS covered area.
- *BTS* - Base Transceiver Station -
- *DC* - Direct Current
- *GNSS* - Global Navigation Satellite System - A satellite navigation system that allows a specialized receive to determine its location on Earth.
- *LED* - Light Emitting Diode - A diode that emitts light.
- *IP Address* - .
- *PCB* - Printed Circuit Board - The board where electronic components are soldered onto and wired through conductive tracks.
- *RRLP* - Radio Resource Location Protocol - The employed protocol in GSM, UMTS and other wireless networks for providing and exchange of geolocation information.
- *SMA* - SubMiniature version A - SMA is a connector used for interconnecting coaxial cables or PCB electronics that work in the frequency range between 0-18 GHz.
- *TIB* - Time Interface Bus - The TIB is used to provide the synchronization of the clock, frequency and frame number between the nanoBTS when operating in a single 2-4 BTS configuration.
- *TRX* -
- *UART* - Universal Asynchronous Receiver Transmitter - A serial communication interface used by computers or other peripheral devices to communicate.
- *UMTS* - Universal Mobile Telecommunications System - Third generation mobile network based on the GSM standards.

Write what an IP address is

11. SUMMARY

Appendix

A. Installation and configuration guide

In order to evaluate the localization system, it is required to install OpenBSC and to modify the proper source files and compile the system. The aim of this section is to describe that process in such detail that the presented material is sufficient to reproduce equivalent or similar results. The guide was successfully tested out on the following operating systems: Ubuntu 10.04 LTS 64 bit and Ubuntu 12.04 LTS 64 bit. A self-bootable test USB system is supplied with the thesis and it can be evaluated without executing the given steps. There is a marking difference between text given in light and dark grey background color, the first ought to be typed in into the terminal window or it may be an output produced by an application, whereas the later emphasizes a file modification case.

A.1. Installation of OpenBSC

In order to compile OpenBSC it is required to install the following precompiled packages[1]:

- libdbi0
- libdbi0-dev
- libdbd-sqlite3
- libortp-dev
- build-essential
- libtool
- autoconf
- automake
- git-core
- pkg-config

[1] If more details are required for the installation process a guide can be found at [33].

Before installing the required packages and libraries, to keep the installation process clean and free of modifying other files, the author will create a new directory.

```
mkdir gsm_localization
cd gsm_localization
```

By executing the following instructions the required libraries will be installed.

```
sudo apt-get install libdbi0-dev libdbd-sqlite3 build-essential
sudo apt-get install libtool autoconf automake git-core
sudo apt-get install pkg-config libortp-dev
```

After the packages were installed, *libosmocore* library must be downloaded, compiled and installed. By executing the following instructions:

```
git clone git://git.osmocom.org/libosmocore.git
cd libosmocore
autoreconf -fi
./configure
make
sudo make install
sudo ldconfig
cd ..
```

In the next step *libosmo-abis* will be installed.

```
git clone git://git.osmocom.org/libosmo-abis.git
cd libosmo-abis
autoreconf -fi
./configure
make
sudo make install
sudo ldconfig
cd ..
```

After the previous steps have finished successfully, the author will proceed with downloading, compiling and installing OpenBSC.

```
git clone git://git.osmocom.org/openbsc.git
cd openbsc/openbsc
autoreconf -i
sudo export PKG_CONFIG_PATH=/usr/local/lib/pkgconfig
./configure
make
```

At this point, OpenBSC should be successfully compiled.

A.2. Configuring nanoBTS for OpenBSC

To enable the nanoBTS and OpenBSC to be fully operational, the last configuration steps have to be made. It is necessary to inform the nanoBTS of the IP address of the server that is running OpenBSC since it must connect to OpenBSC. We need to find a free ARFCN channel where our system is expected to operate[2].

To find the ID and the IP address of the nanoBTS it is required to start *ipaccess-find*[3].

```
cd ~/gsm_localization/openbsc/openbsc/src/ipaccess
./ipaccess-find
```

ipaccess-find will produce an output similar to the one given:

```
Trying to find ip.access BTS by broadcast UDP...
MAC_Address='00:02:95:00:61:70'  IP_Address='132.230.4.63'
Unit_ID='1801/0/0'  Location_1=''  Location_2='BTS_NBT131G'
Equipment_Version='165g029_73'
Software_Version='168a352_v142b30d0'
Unit_Name='nbts-00-02-95-00-61-70'
Serial_Number='00110533'
```

In the next step, the nanoBTS is informed of the OpenBSC IP address by typing the following commands (the first IP address belongs to the server running OpenBSC and the second to the nanoBTS):

```
cd ~/gsm_localization/openbsc/openbsc/src/ipaccess
./ipaccess-config -o 132.230.4.65 132.230.4.63 -r
```

It is required to create the directory where the configuration file will be located and to modify the configuration file.

```
sudo mkdir /usr/local/lcr
cd ~/gsm_localization/openbsc/openbsc/doc/
cd examples/osmo-nitb/nanobts
sudo cp openbsc.cfg /usr/local/lcr
sudo vim /usr/local/lcr/openbsc.cfg
```

[2] A licence has to be obtained from the Federal Network Agency (German: *Bundesnetzagentur*), otherwise it is ilegal and may be considered as a criminal act.

[3] The nanoBTS ought to be blinking in orange color before starting *ipaccess-find*.

A free ARFCN channel can be found using a spectrum analyzer and by setting the frequency range to the GSM frequency band. One has to slide through the frequencies shown on the X-axis, and by looking at the Y-axis with appropriate frequency resolution[4], where the received power is represented[5]. By patiently observing the Y-axis it can be easily seen on the X-axis which channels are taken by other GSM service providers and which are free. The chosen channel ought to be peak free. Once a free frequency channel has been found, it is necessary to instruct the nanoBTS to operate in that frequency range. The line, numbered 58, has to be modified with the correct free ARFCN channel,in this case 877.

```
arfcn 877
```

The ARFCN channel value can be calculated using the given formula in (A.2.1), where f_{start} is the starting frequency of the uplink bandwitdh for DCS1800, f_{CB} is the channel bandwidth and *Offset* is the offset[6].

$$f_{up}(\text{ARFCN}) = f_{start} + f_{CB} \cdot (\text{ARFCN} - \text{Offset})$$

$$where \begin{cases} f_{start} &= 1710.2\,\text{MHz} \\ f_{CB} &= 200\,\text{kHz} \\ \text{Offset} &= 512 \end{cases} \tag{A.2.1}$$

On line numbered 53, the last configuration file modification has to be made for the final configuration of the OpenBSC software. The Unit ID from the output above has to be set[7].

```
ip.access unit_id 1801 0
```

At this point the nanoBTS and OpenBSC configuration is done.

[4] The frequency resolution must be set to $f_{CB} = 200\,\text{kHz}$ or higher values for faster movement in the frequency spectrum.

[5] Dependent of the manufacturer and settings of the spectrum analyzer, it can show signal amplitude, magnitude and power.

[6] A table with frequency channels can be found at the following URL: https://gsm.ks.uni-freiburg.de/arfcn.php

[7] Indentation has to match the one of the configuration file.

A.3. Installation and configuration of GNSS assistance software

To install the RRLP software that generates GNSS assistance data several libraries are required to be installed, *cURL*[8], *libconfig* and *SQLite*. *cURL* was used for the purpose of safely downloading GNSS data from the Navigation Center of the US Coast Guard and Trimble server. *libconfig* library is used for reading in the configuration file, this way compiling of the software whenever one changes the settings was avoided. The *SQLite* library was employed to access the database used by OpenBSC to store the respondence data from the mobile stations.

```
cd ~/gsm_localization
sudo apt-get install libsqlite3-dev
wget http://curl.haxx.se/download/curl-7.25.0.tar.gz
wget http://www.hyperrealm.com/libconfig/libconfig-1.4.8.tar.gz
tar -xvzf curl-7.25.0.tar.gz
tar -xvzf libconfig-1.4.8.tar.gz
cd curl-7.25.0
make
sudo make install
cd ..
cd libconfig-1.4.8/
./configure
make
sudo make install
```

Once the libraries have been successfully installed, the user may proceed with the configuration and compiling the GNSS assistance software, which is the key software produced in this thesis. The configuration file can be found in the same directory as the RRLP modules under the name: "gnssrrlp.cfg". The sample configuration file is already preconfigured for the location of "Angewandte Mathematik und Rechenzentrum" building. Latitude and longitude of the BTS are expressed in decimal degrees and are bounded by $\pm 90°$and $\pm 180°$respectively. Positive latitudes are north of the equator, whereas negative are south of the equator. It is alike for longitude coordinates, positive longitudes are east of Prime Meridian and negative are west of the Prime Meridian. If the position in decimal degrees of the BTS is unknown, it is straightforward to derive them using the formula given in (A.3.1), where D are

[8] It may happen that the given download URLs are wrong and in the meantime have changed, but one can easily find the latest versions on http://curl.haxx.se/ and http://www.hyperrealm.com/libconfig/

degrees, M are minutes and S are seconds[9].

$$DD = D + \frac{M}{60} + \frac{S}{3600} \tag{A.3.1}$$

Describe other parameters as well.

The altitude may be left as it is, set to 0, since it is not used in the current measurement technique[10].

```
// An example configuration file for the GNSS RRLP software.
name = "Configuration for GNSS and RRLP";

// Change the settings if required:
settings =
{
  config = ( {
    ephemeris_url  = "ftp://ftp.trimble.com/pub/eph/CurRnxN.nav";
    almanac_url = "http://www.navcen.uscg.gov/ ↙
       ↳ ?pageName=currentAlmanac&format=yuma";
    latitude_of_BTS  = 48.003601;
    longitude_of_BTS    = 7.848056;
    altitude_of_BTS  = 0.0;
    uncertainty_of_lat_long  = 7;
    uncertainty_of_alt  = 7;
    confidence_level    = 0;
    ephemeris_repair  = false;
    use_reference_time  = false;
    extra_seconds_to_add  = 7;
    timezone_of_BTS  = 1;
    time_to_refresh_ephem = 1;
    time_to_refresh_alm = 1 ; } );
};
```

CHECK IF THIS IS CORRECT

CHECK IF THIS IS CORRECT

The target user, one wants to locate, has to be inside of a geometric estimated shape. This shape can be described using an ellipsoid point with altitude and uncertainty ellipsoid. The uncertainty of the latitude and longitude correctness can be described using equation (A.3.2) [3]. The uncertainty of r is expressed in meters, it defines how accurate is the specified location of the BTS. In the configuration file, K is set to 7, which corresponds to $r = 9.4872$ m. Instead of using the integer parameter

[9] An online converter of the Federal Communication Commission can be used as well to convert from degrees, minutes and seconds to decimal degrees and vice versa http://transition.fcc.gov/mb/audio/bickel/DDDMMSS-decimal.html

[10] If the value is set to zero, it is important to set it to 0.0 because *libconfig* would otherwise convert it to an integer however it is a floating point number.

K as the known variable, the equation (A.3.2) can be rewritten as in (A.3.3), where we can get the integer value K for a previously selected r.

$$r = C((1+x)^K - 1)$$

$$where \begin{cases} C &= 10 \\ x &= 0.1 \\ K &\in [0, 127] \cap \mathbb{N}_0 \end{cases} \tag{A.3.2}$$

$$K = \left\lceil \frac{ln(\frac{r}{C} + 1)}{ln(1+x)} \right\rceil$$

$$where \begin{cases} C &= 10 \\ x &= 0.1 \\ r &\in [0, 1800]\,\text{km} \end{cases} \tag{A.3.3}$$

A set of uncertainties r is given in table A.3.1 for various integer values of K.

Value of K	Value of uncertainty r
0	0 m
1	1 m
2	2.1 m
3	3.3 m
-	-
20	57.3 m
-	-
60	3.0348 km
-	-
100	137.8 km
-	-

Table A.3.1.: Example uncertainties (latitude and longitude) for various integer values of K

Altitude uncertainty can be described using the same Binomial expansion method, as given in (A.3.4), however with altered constant values [3]. The altitude uncertainty ranges between 0 m and 990.5 m ($h \in [0, 990.5]$ m). Although the same constant name K is used, it describes the altitude uncertainty, (A.3.5).

$$h = C((1+x)^K - 1)$$

$$where \begin{cases} C &= 45 \\ x &= 0.025 \\ K &\in [0,127] \wedge \|K\| \end{cases} \tag{A.3.4}$$

$$K = \left\lceil \frac{ln(\frac{h}{C}+1)}{ln(1+x)} \right\rceil$$

$$where \begin{cases} C &= 45 \\ x &= 0.025 \\ h &\in [0,990.5]\,\mathrm{m} \end{cases} \tag{A.3.5}$$

A set of uncertainties h is given in table A.3.2 for various integer values of K.

Value of K	Value of uncertainty h
0	0 m
1	1.13 m
2	2.28 m
3	3.46 m
-	-
20	28.74 m
-	-
60	152.99 m
-	-
100	486.62 m
-	-

Table A.3.2.: Example uncertainties (altitude) for various integer values of K

Confidence level is the next parameter in the configuration file that needs to be set. It can take any integer value between 0 and 127. The confidence level defines the percentage of the confidence that the target entity, the GSM user one wants to locate, is within the geometric shape defined earlier. A value of 0 and between 100 and 127, may be interpreted as "no information" [3]. The reason why the values are not limited to 100 is because of the nature of binary numbers and that 2^6 bits is not sufficient to represent the number 100, but rather requires one bit more.

Confidence level is followed by the ephemeris repair option. Ephemeris repair is a variable of the boolean type, it can take two different values *true* or *false*. Ephemeris

data may contain errors or miss some satellite information [27] [22] and the ephemeris repair function, if set to true, will take data of the previous measurement report. This introduces an error as well.

To increase the speed of measurement report, reference time can be used to provide extra information for the A-GPS in the MS of target entity. This field is of boolean type, if set to true, reference time is included in the sent packets.

Since the sent packets are not transmitted in real time but put on a stack and then sent to the MS, a time delay exists. A solution to this problem is to add extra seconds to the reference time being sent. In order to assess the amount of extra seconds to add, the GSM operator is required experimentally to verify his/her findings. .

see how much the reference time can deviate from current time

The reference time being sent to the MS is Coordinated Universal Time (UTC). The GPS device receives UTC time from the satellites and adjusts the computer time. To set the correct time, time zone offset of the BTS ought to be set correctly.

Finally, the refresh time of downloading new almanac and ephemeris data has to be set. The variable uses the hour unit, how often the data are being downloaded. If the data are used from a local GNSS station, refresh time of the ephemeris data should be set to every 30 minutes or 0.5 hours. The almanac data are valid for up to 180 days [1] but are updated usually every day[11] [18].

[11] Almanac update times can be found here: http://www.navcen.uscg.gov/?pageName=currentNanus&format=txt

B. Sourcecode

Example:

```
#include <stdio.h>

int main(void)
{
    printf("Hallo Welt!\n");
    return 0;
}
```

C. GPS Constants and equations

$$
\begin{aligned}
A &= (\sqrt{A})^2 \\
n_0 &= \sqrt{\frac{\mu}{A^3}} \\
t_k &= t - t_{oe} \\
n &= n_0 + \Delta n \\
M_k &= M_0 + nt_k \\
M_k &= E_k - e\sin E_k \\
v_k &= \tan^{-1}\left(\frac{\sin v_k}{\cos v_k}\right) = \tan^{-1}\left(\frac{\frac{\sqrt{1-e^2}\sin E_k}{1-e\cos E_k}}{\frac{\cos E_k - e}{1-e\cos E_k}}\right) \\
v_k &= \tan^{-1}\left(\frac{\sin v_k}{\cos v_k}\right) = \tan^{-1}\left(\frac{\sqrt{1-e^2}\sin E_k/(1-e\cos E_k)}{(\cos E_k - e)/(1-e\cos E_k)}\right) = \tan^{-1}\left(\frac{\sqrt{1-e^2}\sin E_k}{\cos E_k - e}\right) \\
E_k &= \cos^{-1}\left(\frac{e+\cos v_k}{1+e\cos v_k}\right) \\
\Phi_k &= v_k + \omega \\
\delta u_k &= c_{us}\sin 2\Phi_k + C_{us}\cos 2\Phi_k \qquad \text{(C.0.6)} \\
\delta r_k &= c_{rc}\cos 2\Phi_k + C_{rs}\sin 2\Phi_k \\
\delta i_k &= c_{ic}\cos 2\Phi_k + C_{is}\sin 2\Phi_k \\
u_k &= \Phi_k + \delta u_k \\
r_k &= A(1 - e\cos E_k) + \delta r_k \\
i_k &= i_0 + \delta i_k + (IDOT)t_k \\
x_k^{'} &= r_k\cos u_k \\
y_k^{'} &= r_k\sin u_k \\
\Omega_k &= \Omega_0 + (\Omega - \Omega_e)t_k - \Omega_e t_{oe} \\
x &= x_k^{'}\cos\Omega_k - y_k^{'}\cos i_k\sin\Omega_k \\
y &= x_k^{'}\sin\Omega_k - y_k^{'}\cos i_k\cos\Omega_k \\
z &= y_k^{'}\sin i_k
\end{aligned}
$$

$$
\mu_e = 3.986004418\cdot 10^{14}\frac{m^3}{s^2} \quad \Longleftarrow \quad \text{Geocentric gravitational constant} \qquad \text{(C.0.7)}
$$

$$c = 2.99792458 \cdot 10^8 \frac{m}{s} \quad \Longleftarrow \quad \text{speed of light} \tag{C.0.8}$$

Bibliography

[1] Navstar GPS User Equipment Introduction. Online, Sept. 1996. URL http://www.navcen.uscg.gov/pubs/gps/gpsuser/gpsuser.pdf.

[2] Interface Specification IS-GPS-200. Online, June 2010. URL http://www.losangeles.af.mil/shared/media/document/AFD-100813-045.pdf.

[3] 3GPP-Coordinates. 3GPP TS 23.032 V6.0.0 (2004-12), 3rd Generation Partnership Project; Technical Specification Group Core Network; Universal Geographical Area Description (GAD) (Release 6). Technical report, Dec. 2004.

[4] N. Agarwal, J. Basch, P. Beckmann, P. Bharti, S. Bloebaum, S. Casadei, A. Chou, P. Enge, W. Fong, N. Hathi, W. Mann, A. Sahai, J. Stone, J. Tsitsiklis, and B. Van Roy. Algorithms for GPS operation indoors and downtown. *GPS Solutions*, 6:149–160, 2002. ISSN 1080-5370. 10.1007/s10291-002-0028-0.

[5] D. Akopian and J. Syrjarinne. A network aided iterated LS method for GPS positioning and time recovery without navigation message decoding. In *Position Location and Navigation Symposium, 2002 IEEE*, pages 77–84, 2002. doi: 10.1109/PLANS.2002.998892.

[6] A. Bensky. *Wireless positioning technologies and applications*. Artech House, Boston, Mass, 2008. ISBN 1596931302.

[7] blur group marketing. Trends and Statistics in Location Based Services. http://blur-marketing.com/blog/trends-and-statistics-in-location-based-services/. [Online; accessed 7-July-2012].

[8] K. Borre. *A Software-Defined GPS and Galileo Receiver: A Single-Frequency Approach (Applied and Numerical Harmonic Analysis)*. Birkhäuser Boston, 2006. ISBN 9780817643904.

[9] M. Braasch and A. van Dierendonck. GPS receiver architectures and measurements. *Proceedings of the IEEE*, 87(1):48–64, jan 1999. ISSN 0018-9219. doi: 10.1109/5.736341.

[10] J. R. Clynch. Earth Coordinates. http://www.gmat.unsw.edu.au/snap/gps/clynch_pdfs/coorddef.pdf, 2006. [Online; accessed 27-June-2012].

[11] CORP, DAISHINKU. Development of Miniature High-Precision SMD TCXO for GPS. Technical report, DAISHINKU CORP. 1389 Shinzaike, Hiraoka-cho, Kakogawa, Hyogo 675-0194 Japan, 2008. URL http://www.kds.info/html/products/new_product/4567115_en.htm.

[12] V. Diggelen. *A-GPS assisted GPS, GNSS, and SBAS*. Artech House, Boston, 2009. ISBN 1596933747.

[13] G. Djuknic and R. Richton. Geolocation and assisted GPS. *Computer*, 34(2): 123 –125, feb 2001. ISSN 0018-9162. doi: 10.1109/2.901174.

[14] edited by Mohamed Ibnkahla. *Signal Processing for Mobile Communications Handbook*. CRC Press, 2004. ISBN 084931657X.

[15] C. H. Elliott D. Kaplan. *Understanding GPS: principles and applications*. Artech House, Boston, 2006. ISBN 1580538940.

[16] Email Marketing Reports. Smartphone statistics and market share. http://www.email-marketing-reports.com/wireless-mobile/smartphone-statistics.htm. [Online; accessed 7-July-2012].

[17] GPS World. European Commission Report on Galileo Estimates $ 1 Trillion in Europe Depends on SatNav. http://www.gpsworld.com/gnss-system/news/european-commission-report-galileo-estimates-1-trillion-europe-depends-satnav-10950. [Online; accessed 27-June-2012].

[18] J. G. Grimes. GLOBAL POSITIONING SYSTEM STANDARD POSITIONING SERVICE PERFORMANCE STANDARD. Online, Sept. 2008. URL http://www.gps.gov/technical/ps/2008-SPS-performance-standard.pdf.

[19] GSMA. Brief History of GSM & the GSMA. http://www.gsma.com/history/. [Online; accessed 7-July-2012].

[20] X. Guan, D. Hu, and J. Chen. Design and implementation of the acquisition circuit in software GPS receiver. In *Mobile Technology, Applications and Systems, 2005 2nd International Conference on*, pages 4 pp.–4, nov. 2005. doi: 10.1109/MTAS.2005.243823.

[21] N. Harper. *Server-side GPS and assisted-GPS in Java*. Artech House, Boston, 2010. ISBN 9781607839859.

[22] L. Heng, G. X. Gao, T. Walter, and P. Enge. GPS Ephemeris Error Screening and Results for 2006-2009. *ION Institute of Navigation Global Navigation Satellite Systems Conference*, 2010.

[23] P. A. Iglesias. Linearization. http://www.ece.jhu.edu/~pi/Courses/454/NotesA.pdf. [Online; accessed 27-June-2012].

[24] ip.access ltd. GSM-over-IP picocells for in-building coverage and capacity, 2005. URL http://www.hexazona.com/nexwave/docs/ipaccess/nanoBTS;1800-1900.pdf.

[25] ip.access ltd. The world's most deployed picocell. http://www.ipaccess.com/en/nanoGSM-picocell, 2007. [Online; accessed 3-April-2012].

[26] ip.access ltd. nanoBTS Installation Manual, 2009. URL http://subversion.assembla.com/svn/bxpgfKRFar3O9EeJe5afGb/PP/ipaccess/NGSM_INST_300_nanoBTS_Install_v3_0.pdf.

[27] D. C. Jefferson and Y. E. Bar-Sever. Accuracy and Consistency of Broadcast GPS Ephemeris Data. *ION Institute of Navigation International Technical Meeting*.

[28] P. A. Kline. *Atomic Clock Augmentation For Receivers Using the Global Positioning System*. PhD thesis. URL http://scholar.lib.vt.edu/theses/available/etd-112516142975720/.

[29] K. W. Kolodziej and J. Hjelm. *Local Positioning Systems: LBS Applications and Services*. CRC Press, 2006. ISBN 0849333490.

[30] C. Ma, G. Lachapelle, and M. E. Cannon. Implementation of a Software GPS Receiver. In *Proceedings of ION GNSS 2004 (Session A3), Long Beach, CA*, sep. 2004. URL http://plan.geomatics.ucalgary.ca/papers/04gnss_ion_cmaetal.pdf.

[31] Martin Zwilling, Forbes Magazine. Location-Based Services are a Bonanza for Startups. http://www.forbes.com/sites/martinzwilling/2011/01/31/location-based-services-are-a-bonanza-for-startups/. [Online; accessed 7-July-2012].

[32] T. Ogunfunmi. *Adaptive Nonlinear System Identification: The Volterra and Wiener Model Approaches (Signals and Communication Technology)*. Springer, 2007. ISBN 0387263284.

[33] osmocom. OpenBSC build guide. Web. URL http://openbsc.osmocom.org/trac/wiki/Building_OpenBSC. [Online; accessed 22-May-2012].

[34] PERICOM. Choice of TCXO for GPS Design. Technical report, Pericom Semiconductor Corporation, 3545 North First St., San Jose, CA 95134, USA, 2008. URL http://www.pericom.com/pdf/applications/AN335.pdf.

[35] A. Razavi, D. Gebre-Egziabher, and D. Akos. Carrier loop architectures for tracking weak GPS signals. *Aerospace and Electronic Systems, IEEE Transactions on*, 44(2):697–710, april 2008. ISSN 0018-9251. doi: 10.1109/TAES.2008.4560215.

[36] S. Soliman, S. Glazko, and P. Agashe. GPS receiver sensitivity enhancement in wireless applications. In *Technologies for Wireless Applications, 1999. Digest. 1999 IEEE MTT-S Symposium on*, pages 181–186, feb 1999. doi: 10.1109/MTTTWA.1999.755159.

[37] Spirent Communications. Spirent Expands Leadership in Testing E911 and Location Based Services for LTE Networks. http://www.spirent.com/About-Us/News_Room/Press-Releases/2012/2012_02_21_Spirent_LBS_LTE_Testing. [Online; accessed 7-July-2012].

[38] J. Stewart. *Calculus*. Brooks Cole, 2011. ISBN 0538497815.

[39] The Register, UK News magazine. FCC to fine network operators who can't find customers. http://www.theregister.co.uk/2007/08/31/e911_fine/. [Online; accessed 7-July-2012].

[40] u-blox AG. UBX-G5010, G5000/G0010. http://www.texim-europe.com/promotion/560/ubx-g5010%20datasheet_te.pdf, 2009. [Online; accessed 5-April-2012].

[41] G. Xu. *GPS: Theory, Algorithms and Applications*. Springer, 2007. ISBN 3540727140.

[42] R. M. Zahoransky. Localization in GSM Mobile Radio Networks. Master's thesis, University of Freiburg, 2011.

[43] V. Zeimpekis, G. M. Giaglis, and G. Lekakos. A taxonomy of indoor and outdoor positioning techniques for mobile location services. *SIGecom Exch.*, 3(4):19–27, Dec. 2002. ISSN 1551-9031. doi: 10.1145/844351.844355. URL http://doi.acm.org/10.1145/844351.844355.