Examensarbete utfört i Kommunikationssystem vid Tekniska högskolan vid Linköpings universitet av

Andreas Nordzell

LiTH-ISY-EX--13/4681--SE

Linköping 2013

Department of Electrical Engineering Linköpings tekniska högskola
Linköpings universitet Linköpings universitet
SE-581 83 Linköping, Sweden 581 83 Linköping
Double Differential TOA Positioning for GSM

Examensarbete utfört i Kommunikationssystem
vid Tekniska högskolan vid Linköpings universitet
av
Andreas Nordzell

LiTH-ISY-EX--13/4681--SE

Handledare: Mirsad Čirkić, Doktorand
ISY, Linköpings universitet
Anders Johansson, PhD
FOI

Examinator: Danyo Danev
ISY, Linköpings universitet

Linköping, 17 juni 2013
Dubbel Differential TOA Positioning for GSM

For most time-based positioning techniques, synchronization between the objects in the system is of great importance. GPS (global positioning system) signals have been found very useful in this area. However, there are some shortcomings of these satellite signals, making the system vulnerable. The aim of this master thesis is to investigate an alternative method for synchronization, independent of GPS signals, which could be used as a complement. The proposed method takes advantage of the broadcast signals from telecommunication towers, and use them for calculation of the synchronization error between two receivers. By looking at the time difference between arrival times at the receivers, and compare it to the true time difference, the synchronization error can be found. A precondition is that the locations of the receivers as well as the tele tower are known beforehand, so that the true time difference can be calculated using geometry.

The arrival times are determined through correlation between the received signals and known training bits, which are a part of the transmission sequence. For verification, experiments were made on localization of a mobile phone in the GSM (global system of mobile communications) network.

This research was a collaboration with FOI, the Swedish Defense Research Agency, where most of the work was done.
Till Maja, Sanna, Jonas, Vedran, Björn och Johan.
Utan er hade det nog gått ändå...
Abstract

For most time-based positioning techniques, synchronization between the objects in the system is of great importance. GPS (global positioning system) signals have been found very useful in this area. However, there are some shortcomings of these satellite signals, making the system vulnerable. The aim of this master thesis is to investigate an alternative method for synchronization, independent of GPS signals, which could be used as a complement. The proposed method takes advantage of the broadcast signals from telecommunication towers, and use them for calculation of the synchronization error between two receivers. By looking at the time difference between arrival times at the receivers, and compare it to the true time difference, the synchronization error can be found. A precondition is that the locations of the receivers as well as the tele tower are known beforehand, so that the true time difference can be calculated using geometry.

The arrival times are determined through correlation between the received signals and known training bits, which are a part of the transmission sequence. For verification, experiments were made on localization of a mobile phone in the GSM (global system of mobile communications) network.

This research was a collaboration with FOI, the Swedish Defense Research Agency, where most of the work was done.
Acknowledgments

My sincere and most grateful thank you goes to ...

...my supervisor Anders Johansson and project manager Patrik Hedström at FOI, for the countless hours you have spent helping me through insightful discussions, with cables and wires, with report reflections and last but not least, to execute the field experiment. Without your help and support, I would never have reached my goal.

...my supervisor Mirsad Čirkić, for constructive critics during the work with this report, as well as the long repetition course in Gaussian distribution calculations and the Q-function.

...my examiner Danyo Danev, for many inspiring courses in the field of communication systems, and for helping me become a Master of science in Applied Physics and Electrical Engineering.

Linköping, June 2013
Andreas Nordzell
# Content

## Symbols

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>xi</td>
<td></td>
</tr>
</tbody>
</table>

## Abbreviations

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>xiii</td>
<td></td>
</tr>
</tbody>
</table>

## 1 Introduction

1.1 Thesis Description .......................... 1
1.2 Synchronization and the Importance of Accuracy ........ 2
1.3 Restrictions .................................. 3
1.4 The Matter of No GPS .......................... 3
1.5 Previous Work ................................ 3
1.6 Outline ...................................... 4

## 2 Theory

2.1 GSM ........................................... 5
2.1.1 General Information ......................... 5
2.1.2 Transmission Rate and Bandwidth ............. 5
2.1.3 Time Division Multiple Access ................ 7
2.1.4 Frame Structure ............................ 7
2.1.5 Burst Structure ............................ 7
2.1.6 Frequency Hopping .......................... 8
2.1.7 Transmission and Reception .................. 8
2.1.8 Modulation ................................. 9
2.1.8.1 Gaussian Minimum Shift Keying ............ 9
2.1.8.2 Differential Encoding .................... 9
2.1.8.3 Gaussian Filtering ....................... 10
2.1.8.4 Phase Function .......................... 10
2.1.9 Relevant Information ....................... 11
2.1.10 Training Sequences ......................... 11

2.2 Time-Based Localization ....................... 12
2.2.1 Time Difference of Arrival .................. 12
2.2.2 Time of Arrival ............................ 13
2.2.3 Double Differential Time of Arrival .......... 14
2.2.3.1 Calculating the Time Difference .......... 15
2.2.3.2 Evaluation of Bound for Synchronization Error . . 16

3 Method 19
3.1 Correlation ........................................ 19
   3.1.1 Mathematical Description ....................... 20
   3.1.2 Comments on Accuracy .......................... 22
3.2 Curve Fitting ...................................... 23
3.3 Averaging .......................................... 23
3.4 Implementation ..................................... 23
   3.4.1 Demodulation and Frequency Correction ............ 23
   3.4.2 Practical Aspects ............................... 24
   3.4.3 Discrete Correlation ............................ 24
   3.4.4 Interpolation .................................. 25
   3.4.5 Modulated Training Sequence .................... 25
   3.4.6 Algorithms .................................. 26

4 Simulation 29
4.1 System Model ..................................... 29
4.2 Calculations ...................................... 29
4.3 Results .......................................... 31

5 Laboratory Trials and Field Test 37
5.1 Receiver Hardware .................................. 37
5.2 TEMS Mobile Phone ................................. 38
5.3 Execution ......................................... 38
   5.3.1 Laboratory Setup ................................ 40
   5.3.2 Field Test Setup ............................... 41
5.4 Results .......................................... 43
   5.4.1 Received Signals ............................... 43
   5.4.2 Laboratory Trials ............................... 43
   5.4.3 Field Test .................................. 47
   5.4.4 Comments on Results ........................... 48

6 Conclusions 53
6.1 Results .......................................... 53
6.2 Suggested Improvements ........................... 53
6.3 Future Developments ............................... 54
6.4 Final Comments .................................. 54

List of Figures 55
List of Tables 58
Bibliography 59
Symbols

In order of appearance

<table>
<thead>
<tr>
<th>Notation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>$s(t)$</td>
<td>Signal sent</td>
</tr>
<tr>
<td>$t, \tau$</td>
<td>Time variable</td>
</tr>
<tr>
<td>$E_b$</td>
<td>Bit (symbol) energy</td>
</tr>
<tr>
<td>$T$</td>
<td>Symbol period ($\approx 3.69$ microseconds)</td>
</tr>
<tr>
<td>$f_c$</td>
<td>Carrier frequency</td>
</tr>
<tr>
<td>$\varphi(t)$</td>
<td>Phase function</td>
</tr>
<tr>
<td>$b$</td>
<td>Information bit</td>
</tr>
<tr>
<td>$d$</td>
<td>Differential encoded bit</td>
</tr>
<tr>
<td>$\alpha$</td>
<td>Information symbol</td>
</tr>
<tr>
<td>$i, j$</td>
<td>Index</td>
</tr>
<tr>
<td>$g(t)$</td>
<td>Gaussian filter (frequency function)</td>
</tr>
<tr>
<td>$h(t)$</td>
<td>Gaussian distribution</td>
</tr>
<tr>
<td>$\text{rect}(t)$</td>
<td>Rectangle function</td>
</tr>
<tr>
<td>$\exp(t)$</td>
<td>Exponential function</td>
</tr>
<tr>
<td>$\sigma$</td>
<td>Standard deviation</td>
</tr>
<tr>
<td>$B_h$</td>
<td>3 dB bandwidth of $h(t)$</td>
</tr>
<tr>
<td>$\mu$</td>
<td>Modulation index</td>
</tr>
<tr>
<td>$w$</td>
<td>White Gaussian noise</td>
</tr>
<tr>
<td>$x(t)$</td>
<td>Received signal</td>
</tr>
<tr>
<td>$\Delta, \delta$</td>
<td>Time delay</td>
</tr>
<tr>
<td>$r(\tau)$</td>
<td>Cross correlation function</td>
</tr>
<tr>
<td>$S(f)$</td>
<td>Cross spectra</td>
</tr>
<tr>
<td>$E[\cdot]$</td>
<td>Expected value</td>
</tr>
<tr>
<td>$\mathcal{F}[\cdot]$</td>
<td>Fourier transform</td>
</tr>
<tr>
<td>$f$</td>
<td>Frequency variable</td>
</tr>
<tr>
<td>$c$</td>
<td>Propagation speed of light in air</td>
</tr>
<tr>
<td>$P_x$</td>
<td>Position of object X</td>
</tr>
<tr>
<td>Notation</td>
<td>Description</td>
</tr>
<tr>
<td>----------</td>
<td>-------------</td>
</tr>
<tr>
<td>MS</td>
<td>Mobile station (transmitter to be located)</td>
</tr>
<tr>
<td>BS</td>
<td>Base station (reference source)</td>
</tr>
<tr>
<td>RX1</td>
<td>Receiver 1</td>
</tr>
<tr>
<td>RX2</td>
<td>Receiver 2</td>
</tr>
<tr>
<td>$\rho$</td>
<td>Circle radius</td>
</tr>
<tr>
<td>$\hat{\tau}_{x,y}$</td>
<td>The time instant for when a signal sent from object $x$ arrives at object $y$ (Time Of Arrival)</td>
</tr>
<tr>
<td>$T_P$</td>
<td>Time period between two consecutive training sequences</td>
</tr>
<tr>
<td>$\epsilon_{SYNC}$</td>
<td>Synchronization error</td>
</tr>
<tr>
<td>$y(t)$</td>
<td>Random signal</td>
</tr>
<tr>
<td>$L$</td>
<td>Length of a training sequence</td>
</tr>
<tr>
<td>$B$</td>
<td>Bandwidth</td>
</tr>
<tr>
<td>$\text{sinc}(t)$</td>
<td>Sinc function (normalized)</td>
</tr>
<tr>
<td>$a$</td>
<td>Constant</td>
</tr>
<tr>
<td>$M$</td>
<td>Number of TOA estimations used for averaging</td>
</tr>
<tr>
<td>$\hat{r}[n]$</td>
<td>Discrete time estimation of the cross correlation function</td>
</tr>
<tr>
<td>$n$</td>
<td>Discrete time variable</td>
</tr>
<tr>
<td>$N$</td>
<td>Number of recorded samples</td>
</tr>
<tr>
<td>$\sigma_2$</td>
<td>Standard deviation</td>
</tr>
<tr>
<td>$\Lambda$</td>
<td>Oversampling rate</td>
</tr>
<tr>
<td>$x_{TR}[n]$</td>
<td>Complex baseband representation of the modulated training sequence</td>
</tr>
<tr>
<td>$j$</td>
<td>Imaginary unit ($j^2 = -1$)</td>
</tr>
<tr>
<td>$f_{OFFSET}$</td>
<td>Frequency offset</td>
</tr>
<tr>
<td>$\hat{x}[n]$</td>
<td>Training sequence with added WGN</td>
</tr>
<tr>
<td>$\hat{\epsilon}_{\text{ERROR}}$</td>
<td>TOA error</td>
</tr>
<tr>
<td>$\hat{\epsilon}_{\text{TOA}}$</td>
<td>RMS for the TOA estimation</td>
</tr>
<tr>
<td>$N_{\text{EST}}$</td>
<td>Number of estimations used for a RMS calculation</td>
</tr>
<tr>
<td>$\Delta_{\text{ERROR}}$</td>
<td>DDTOA error</td>
</tr>
<tr>
<td>$\xi$</td>
<td>Normal distribution variable</td>
</tr>
<tr>
<td>$\chi$</td>
<td>Normal distribution variable</td>
</tr>
<tr>
<td>$\hat{\epsilon}_{\text{DDTOA}}$</td>
<td>RMS for the DDTOA estimation</td>
</tr>
<tr>
<td>$F_d$</td>
<td>Downlink carrier frequency</td>
</tr>
<tr>
<td>$F_s$</td>
<td>Sample frequency</td>
</tr>
<tr>
<td>$F_u$</td>
<td>Uplink carrier frequency</td>
</tr>
</tbody>
</table>
# Abbreviations

In alphabetic order

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AM</td>
<td>Amplitude Modulation</td>
</tr>
<tr>
<td>ALE</td>
<td>Adaptive Line Enhancer</td>
</tr>
<tr>
<td>AOA</td>
<td>Angle Of Arrival</td>
</tr>
<tr>
<td>ARFCN</td>
<td>Absolute Radio Frequency Channel Number</td>
</tr>
<tr>
<td>AWGN</td>
<td>Addative White Gaussian Noise</td>
</tr>
<tr>
<td>A/D</td>
<td>Analog/Digital</td>
</tr>
<tr>
<td>BCC</td>
<td>Base station Color Code</td>
</tr>
<tr>
<td>BSIC</td>
<td>Base Station Identity Code</td>
</tr>
<tr>
<td>CCH</td>
<td>Control Channel</td>
</tr>
<tr>
<td>CPM</td>
<td>Continuous Phase Modulation</td>
</tr>
<tr>
<td>DDC</td>
<td>Digital Downconverter</td>
</tr>
<tr>
<td>DDTOA</td>
<td>Double Differential Time Of Arrival (!)</td>
</tr>
<tr>
<td>DL</td>
<td>Downlink</td>
</tr>
<tr>
<td>DTOA</td>
<td>Differential Time Of Arrival</td>
</tr>
<tr>
<td>EDGE</td>
<td>Enhanced Data rates for GSM evolution</td>
</tr>
<tr>
<td>ETSI</td>
<td>European Telecommunications Standards Institute</td>
</tr>
<tr>
<td>FCCH</td>
<td>Frequency Correction Channel</td>
</tr>
<tr>
<td>FN</td>
<td>TDMA Frame Number</td>
</tr>
<tr>
<td>FOI</td>
<td>Totalförsvarets Forskningsinstitut (Swedish Defense Research Agency)</td>
</tr>
<tr>
<td>GMSK</td>
<td>Gaussian Minimum Shift Keying</td>
</tr>
<tr>
<td>GPRS</td>
<td>General Packet Radio Service</td>
</tr>
<tr>
<td>GPS</td>
<td>Global Positioning System</td>
</tr>
<tr>
<td>GSM</td>
<td>Global System of Mobile communication</td>
</tr>
<tr>
<td>I</td>
<td>Idle</td>
</tr>
<tr>
<td>IF</td>
<td>Intermediate Frequency</td>
</tr>
<tr>
<td>I/Q</td>
<td>In-phase/Quadrature-phase</td>
</tr>
<tr>
<td>Acronym</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>------------------------------</td>
</tr>
<tr>
<td>LOS</td>
<td>Line Of Sight</td>
</tr>
<tr>
<td>NCC</td>
<td>Network Color Code</td>
</tr>
<tr>
<td>PPS</td>
<td>Pulse Per Second</td>
</tr>
<tr>
<td>RF</td>
<td>Radio Frequency</td>
</tr>
<tr>
<td>RMS</td>
<td>Root Mean Square error</td>
</tr>
<tr>
<td>RSS</td>
<td>Received Signal Strength</td>
</tr>
<tr>
<td>SCH</td>
<td>Synchronization Channel</td>
</tr>
<tr>
<td>SNR</td>
<td>Signal to Noise Ratio</td>
</tr>
<tr>
<td>TDMA</td>
<td>Time Division Multiple Access</td>
</tr>
<tr>
<td>TDOA</td>
<td>Time Difference Of Arrival</td>
</tr>
<tr>
<td>TEMS</td>
<td>Test Mobile System</td>
</tr>
<tr>
<td>TOA</td>
<td>Time Of Arrival</td>
</tr>
<tr>
<td>TS0</td>
<td>Time Slot 0 in a TDMA frame</td>
</tr>
<tr>
<td>UL</td>
<td>Uplink</td>
</tr>
<tr>
<td>UWB</td>
<td>Ultra-Wideband</td>
</tr>
</tbody>
</table>
Introduction

Everybody who has been trying to find their way in an unfamiliar city by car, knows how useful it can be with a GPS (global positioning system) device. It is easy to update the map, and you don’t have to stop every other turn to have a look at your directions. However, what happens when you drive into a tunnel? The author certainly knows from a few years back when he was working in Oslo, the capital of Norway, as a delivery man. Oslo has a lot of long tunnels with many different exit points. And how will you know what exit to take when the GPS stops working as soon as you get underground? This is not the question to be answered in this master thesis, yet, it gives a good example of one of the shortcomings of a GPS; namely the importance of a line of site (LOS) signal from the satellites. It can be difficult to use a GPS device indoor, or even in an urban environment with a lot of adjacent buildings and high skyscrapers.

From an electronic warfare point of view, which is the main field for this master thesis, the GPS signals can also easily be jammed or "spoofed" by the enemy. This can cause trouble with self-positioning and time synchronization.

This master thesis will be dealing with the troubles of time synchronization when trying to localize the origin of a radio signal. The time difference of arrival (TDOA) system normally use GPS signals for synchronization of the receivers. Here, a variation of TDOA will be introduced and analyzed, that uses signals of opportunity instead of a GPS for time synchronization.

1.1 Thesis Description

The system setup can be seen in Figure 1.1. It consists of two receivers, one reference source and one transmitter to be located. More precise, the target in this
case will be a mobile phone, and the reference source is a telecommunications tower (base station). The goal will be to find the location of the mobile using the difference in time of arrival (TOA)\(^1\) at the receivers. Signals from the telecommunications tower will be used for the synchronization. More on this in Section 2.2.

The signals will be analyzed in the global system for mobile communication (GSM) standard. The reason for this choice over the maybe more up to date choices 3G or 4G is due to the authors prior knowledge of GSM, and also because of its less complex structure.

The exact location will not be of interest, instead only the hyperbola (Section 2.2) of possible positions will be calculated and the positioning error will be examined with respect to this curve.

### 1.2 Synchronization and the Importance of Accuracy

Since radio signals are traveling in the speed of light in air, it is easy to show the importance of accurate calculations of the time differences and thereby the time of arrival. The same argument also explains the reason for the time synchronization. This will be illustrated with an example.

---

#### 1.1 Example

Imagine that two receivers, A and B, are located 400 m apart, and the mobile 300 m away from A in an orthogonal direction of B. The distance to B is then 500 m by Pythagoras’. The difference in distance is 200 m, and the time difference approximately 0.67 µs when dividing by the speed of light. This indicates that an error in time of arrival by the size of only 0.1 µs is enough to end up far from the true difference in distance.

---

\(^1\)TOA means the time instant (or time stamp) for when the signal is detected at the receiver.
How accurate one can determine the time of arrival is a matter of available bandwidth, the signal to noise ratio (SNR), the length of the signal and the receiver hardware. More on this in Chapter 3.

### 1.3 Restrictions

The system will only deal with the direct LOS signals. The reflected ones, as well as the attenuation factor, will be considered as noise in the model. Moreover, all positions, except for the transmitter, are assumed to be known beforehand. They are also seen as stationary, meaning, none of the objects in the system are moving.

Calculations of the time differences will not be done in real time, making the matter of fast and efficient algorithms less important. The signals will be stored on file, and then processed. In an actual electronic warfare situation, the communication between the two receivers (or between a receiver and a third party) are supposed to be minimal. This fact is noted, but will not be of great importance from a practical point of view.

### 1.4 The Matter of No GPS

Although the whole point of this master thesis is to reduce the dependency of a GPS for time synchronization, the GPS will be used when collecting data during the field test. First, to determine the exact location of the receivers, the reference source and also for verification of the mobile position. Second, to be able to analyze the accuracy of the calculations.

The author is well aware of the irony in this, but the use of a GPS simplifies the work a lot. Approaches on self-positioning without GPS can be found in [Vidyarthi, 2012] or [Yan and Fan, 2008].

### 1.5 Previous Work

A large number of articles and technical reports have been written in the field of localization techniques. In [Gustafsson and Gunnarsson, 2005], the most common methods, such as TOA, TDOA, angle of arrival (AOA) or received signal strength (RSS), are briefly described and compared. The article is a few years old, but gives a good overview of mobile positioning, both in the static and in the dynamic case (through filter estimation). [Gezici et al., 2005] also gives a good general description (although in Ultra-wideband (UWB) systems), along with some performance bounds.

[Shahabi et al., 2011] show a way of improving the performance in a TDOA system, by the use of an adaptive line enhancer (ALE). ALE is a way of reducing the noise and thereby increasing the SNR.

In [Yan and Fan, 2008], a way of co-locating a number of asynchronous receivers
is presented. This TDOA system is also independent of GPS and relies on signals of opportunity. The performance is tested using both digital TV signals and AM (amplitude modulation) signals as a reference source.

As a contrast to the asynchronous systems, [Yoon et al., 2012] presents a method for synchronizing the receivers in a TDOA system. This method uses a GPS together with high performance oscillators and efficient signal processing to create precise time synchronization. This article can be good for comparing synchronized and non-synchronized systems.

1.6 Outline

After this introduction, an overview of GSM is presented. It describes the necessary parts for this thesis work. Chapter 2 also includes the theory behind the positioning system, together with the equation used to calculate the time delay between the two receivers. Chapter 3 continues by describing the methods to calculate the time of arrivals, and how to implement them. In Chapter 4, some simulation results are presented. These, quite simple, simulations were made mostly in order to test the methods. The laboratory trials and the field test are introduced in Chapter 5. It describes the equipment that was used and the setup, together with the outcome and comments on the results. The final chapter summarizes the thesis, and a short section is given about the future work.
This chapter describes the necessary theory. To start with, the basics of the GSM protocol is presented, followed by different approaches on time-based localization.

2.1 GSM

In order to determine the time of arrivals, some basic knowledge about the GSM protocol is needed, which will be presented in this section. It includes the parts of GSM that are closely related to the theory behind and implementation of this master thesis. The chapter should be considered as background information to help understand the rest of the thesis. Sections 2.1.9 and 2.1.10 are of special interest. For a deeper insight in GSM, see [3GPP, 2013].

2.1.1 General Information

The global standard for mobile communications, originally groupe spécial mobile, is the second generation protocol for mobile cellular networks. It was developed by the european telecommunications standards institute (ETSI) in the late 80’s and 90’s, to replace the analog first generation standard with a digital one. It was later expanded to include data communications via GPRS (general packet radio service) and EDGE (enhanced data rates for GSM evolution).

2.1.2 Transmission Rate and Bandwidth

The rate for which information is sent is 260’833 symbols/s, and the available bandwidth is 200 kHz per carrier [3GPP, 2013].
Figure 2.1: (a) An overview of the frame structure of GSM. (b) Every 0'th slot in each TDMA frame is put together to create one control channel (CCH) multiframe. F = FCCH burst, S = SCH burst and I = Idle.
2.1.3 Time Division Multiple Access

The access scheme used in GSM is time division multiple access (TDMA). Each TDMA frame contains eight physical channels (or time slots) per carrier. One time slot has a duration of 15/26 ms (≈ 576.9 µs), and includes 156.25 symbols (in this case the same as bits, and the 1/4 bit is included in the guard period). These 156.25 bits are put together in a bit frame, known as a burst.

2.1.4 Frame Structure

The longest cycle of TDMA frames is called a hyperframe, and lasts for 3 h 28 min 53 s and 760 ms. This hyperframe is divided into 2 715 648 TDMA frames, each with a specific TDMA frame number (FN).

The hyperframe contains 2048 superframes, which in turn contains 26 (51-frame) multiframes for the control channel and 51 (26-frame) multiframes for the traffic channels. The multiframes includes 51 respectively 26 TDMA frames. An overview of this can be seen in Figure 2.1a.

The control channel is always located on the first time slot of the TDMA frame, often referred to as TS0. 51 consecutive TS0's create the control channel (CCH) multiframe. The structure of this multiframe can be seen in Figure 2.1b. The important parts for this project are the frequency correction channel (FCCH) burst and the synchronization channel (SCH) burst. There are five of each in one CCH multiframe.

2.1.5 Burst Structure

There are three different kind of bursts of relevance: the FCCH burst, SCH burst and the normal burst. The first two are used in parts of the downlink (from base station to mobile) broadcast communication, and the last one on the traffic channel. All of them consist of 148 bits of information plus a guard period corresponding to 8.25 bits in time (the time it takes to transmit 8.25 bits).

The FCCH burst contains 142 consecutive zeros, apart from the tailbits, which creates a pure sine after modulation. This burst is used to correct for the frequency offset, which can be induced by the receiver hardware. See Figure 2.2.

The structure of the SCH burst can be seen in Figure 2.3. This burst is used for time synchronization between the mobile and the base station. The data part contains information about the FN and also the BSIC (Section 2.1.9). The training

![Figure 2.2: Structure of an FCCH burst.](image-url)
sequence here will also be used when calculating the time of arrival of the down-
link reference signal.

The structure of the normal burst is similar to that of the SCH burst, but with a
shorter training sequence and longer data sequences. See Figure 2.4. This train-
ing sequence will be used when calculating the time of arrival for the signal from
the mobile station.

2.1.6 Frequency Hopping

Frequency hopping can be used optionally in GSM. This is determined by the
operators. The hopping is a predetermined sequence of shifts in carrier frequency.
Each jump is made in the guard period between two time slots.

Frequency hopping will not be relevant for the time of arrival calculations, it is
only mentioned as a fact to help understand the appearance of the signals. As
will be seen in Chapter 5, sampling will only be done for one carrier frequency
per phone call.

2.1.7 Transmission and Reception

The two most common frequency bands for GSM communication are the GSM 900
and GSM 1800. For GSM 900, the downlink carrier frequency is in the band of
935-960 MHz, and uplink (from mobile to base station) communication is be-
tween 890-915 MHz. For GSM 1800, the system operates in 1805-1880 MHz for
downlink, and 1710-1785 MHz for uplink.

Each carrier frequency is separated by 200 kHz, creating 124 different frequency
channels for GSM 900 and 374 channels for GSM 1800. The channel number
is called Absolute Radio Frequency Channel Number (ARFCN). An overview is
given in Table 2.1.

Further on in this report, when mentioning for example "channel 45", it will refer
to ARFCN 45.

Figure 2.3: Structure of an SCH burst.

Figure 2.4: Structure of a normal burst.
Table 2.1: Frequency bands for GSM 900 and GSM 1800.

<table>
<thead>
<tr>
<th>GSM</th>
<th>ARFCN</th>
<th>Uplink [MHz]</th>
<th>Downlink [MHz]</th>
</tr>
</thead>
<tbody>
<tr>
<td>900</td>
<td>$1 \leq i \leq 124$</td>
<td>$890 + 0.2 \cdot i$</td>
<td>Uplink + 45</td>
</tr>
<tr>
<td>1800</td>
<td>$512 \leq i \leq 885$</td>
<td>$1710.2 + 0.2 \cdot (i - 512)$</td>
<td>Uplink + 95</td>
</tr>
</tbody>
</table>

2.1.8 Modulation

The modulation technique most frequently used in GSM is Gaussian minimum shift keying (GMSK). This section gives a brief introduction to GMSK along with the GSM specified parameters, and also the symbol mapping. Later on, in Chapter 3, a derivation of a more implementation-friendly expression for the phase function $\varphi(t)$ will be given.

2.1.8.1 Gaussian Minimum Shift Keying

GMSK is a type of continuous phase modulation (CPM). The general appearance of such signals is

$$s(t) = \sqrt{\frac{2E_b}{T}} \cos(2\pi f_c t + \varphi(t))$$

where $E_b$ is the bit (symbol) energy, $T$ the bit period, $f_c$ the carrier frequency and $\varphi(t)$ the phase function. What $\varphi(t)$ looks like depends on the type of CPM. Gaussian MSK differs from normal MSK by passing the modulated data through a filter with a Gaussian impulse response. This is done to reduce the sidelobe levels in its power spectral density function.

GMSK is an attractive modulation scheme due to its power and spectral efficiency [Ahlin and Zander, 1996]. However, it introduces intersymbol interference. More on CPM and GMSK can be found in [Ahlin and Zander, 1996; Madhow, 2008].

2.1.8.2 Differential Encoding

The first step of the modulation process is differential encoding. The bits $b_i \in \{0, 1\}$ in a burst are encoded as

$$d_i = b_i \oplus b_{i-1} \quad (d_i \in \{0, 1\})$$

where $< \oplus >$ denotes addition modulo 2 [3GPP, 2013]. The differential encoded bits are then mapped onto symbols according to

$$\alpha_i = 1 - 2d_i \quad (\alpha_i \in \{-1, 1\})$$

where $\alpha_i$ is the input to the modulator.
2.1.8.3 Gaussian Filtering

The Gaussian filter $g(t)$ is defined by

$$g(t) = h(t) \star \text{rect}\left(\frac{t}{T}\right)$$

where $\star$ means convolution and \text{rect} is the normal 'box' function defined as

$$\text{rect}\left(\frac{t}{T}\right) = \begin{cases} \frac{t}{T} & \text{for } |t| \leq \frac{T}{2} \\ 0 & \text{otherwise} \end{cases}$$

The impulse response $h(t)$ is a Gaussian distribution according to

$$h(t) = \frac{\exp\left(-\frac{t^2}{2(\sigma T)^2}\right)}{\sqrt{2\pi} \cdot \sigma T}$$

where

$$\sigma = \frac{\sqrt{\ln 2}}{2\pi B_h T}$$

and $B_h$ is the 3 dB bandwidth of the filter with impulse response $h(t)$. For GSM, $B_h T = 0.3$.

2.1.8.4 Phase Function

The output phase of the modulated sequence is given by

$$\varphi(t) = \sum_i \alpha_i \mu \pi \int_{-\infty}^{t+iT} g(\tau) d\tau$$

where the modulating index $\mu = 0.5$, which gives a maximum change in phase of $\pi/2$ between two consecutive symbol periods. The time instant $t = 0$ refers to the start of the symbol period for the first tail bit in a burst. Since it is impossible to know which data bits are sent beforehand, there will be a random phase offset between the received training sequence and the modulated version that is used for correlation.

The above described signal $s(t)$ is the analog passband version of the sent signal. However, the signal processing on the receiver side will be done on the digital complex baseband version.
Table 2.2: List of different possible training sequences depending on BCC [3GPP, 2013].

<table>
<thead>
<tr>
<th>BCC</th>
<th>Training Sequence</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>(0,0,1,0,0,1,0,1,1,0,0,0,1,0,0,0,1,0,0,1,0,1,1,1)</td>
</tr>
<tr>
<td>1</td>
<td>(0,0,1,0,1,1,0,1,1,0,1,1,0,0,0,1,0,1,0,1,1,1,1)</td>
</tr>
<tr>
<td>2</td>
<td>(0,1,0,0,0,1,1,0,1,1,0,1,0,0,1,0,0,0,1,0,0,0,1,0,1,1,0)</td>
</tr>
<tr>
<td>3</td>
<td>(0,1,0,0,0,1,1,1,0,1,1,1,0,1,0,0,0,1,0,0,0,1,1,1,0)</td>
</tr>
<tr>
<td>4</td>
<td>(0,0,0,1,1,0,1,0,1,1,1,0,0,1,0,0,0,0,0,1,1,0,1,1,1)</td>
</tr>
<tr>
<td>5</td>
<td>(0,1,0,0,1,1,0,1,0,1,1,0,0,0,0,1,0,0,1,1,1,0,1,1,0)</td>
</tr>
<tr>
<td>6</td>
<td>(1,0,1,0,0,1,1,1,1,0,1,0,0,1,0,0,1,0,1,0,1,1,1,1)</td>
</tr>
<tr>
<td>7</td>
<td>(1,1,1,0,1,1,1,1,0,0,0,1,0,0,1,0,1,1,1,1,1,1,0,0)</td>
</tr>
</tbody>
</table>

2.1.9 Relevant Information

Within the data part of the SCH burst (see Figure 2.3), there is some information which can be useful when trying to find the time of arrivals. After demodulation and decoding, one can retrieve the TDMA frame number (FN) and the base station identity code (BSIC) [3GPP, 2013]. FN tells you which TDMA frame your SCH burst belongs to (i.e. TS0 in that TDMA frame). This number can be used to make sure that both receivers correlate with the same training sequence, if the synchronization error is assumed relatively large.

The BSIC consists of two separate, 3-bit parts: the network color code (NCC) and the base station color code (BCC). The primary purpose of these color codes is to distinguish between different operators and base stations if they transmit on the same frequency. However, in this case, the BCC information is used to determine which training sequence is used in the normal burst.

2.1.10 Training Sequences

There are eight different training sequences that can be used, depending on operator and base station. These are listed in Table 2.2.

The longer training sequence used in the SCH burst look like:

\[(1,0,1,1,1,0,0,1,0,1,1,0,0,0,1,0,0,1,0,0,1,0,0,1,0,1,0,1,0,1,0,1,1,0,0,1,0,1,0,1,0,1,0,1,0,0,0,1,0,0,1,0,0,1,0,0,1,0,0,1,0,0,1,0,0,1,0,0,1,0,0,1,0,0,1,0,0,1,0,0,1,0,0,1,0,0,1,0,0,1,0,0,1,0,0,1,0,0,1,0,0,1,0,0,1,0,0,1,0,0,1,0,0,1,0,0,1,0,0,1,0,0,1,0,0,1,0,0,1,0,0,1,0,0,1,0,0,1,0,0,1,0,0,1,0,0,1,0,0,1,0,0,1,0,0,1,0,0,1,0,0,1,0,0,1,0,0,1,0,0,1,0,0,1,0,0,1,0,0,1,0,0,1,0,0,1,0,0,1,0,0,1,0,0,1,0,0,1,0,0,1,0,0,1,0,0,1,0,0,1,0,0,1,0,0,1,0,0,1,0,0,1,0,0,1,0,0,1,0,0,1,0,0,1,0,0,1,0,0,1,0,0,1,0,0,1,0,0,1,0,0,1,0,0,1,0,0,1,0,0,1,0,0,1,0,0,1,0,0,1,0,0,1,0,0,1,0,0,1,0,0,1,0,0,1,0,0,1,0,0,1,0,0,1,0,0,1,0,0,1,0,0,1,0,0,1,0,0,1,0,0,1,0,0,1,0,0,1,0,0,1,0,0,1,0,0,1,0,0,1,0,0,1,0,0,1,0,0,1,0,0,1,0,0,1,0,0,1,0,0,1,0,0,1,0,0,1,0,0,1,0,0,1,0,0,1,0,0,1,0,0,1,0,0,1,0,0,1,0,0,1,0,0,1,0,0,1,0,0,1,0,0,1,0,0,1,0,0,1,0,0,1,0,0,1,0,0,1,0,0,1,0,0,1,0,0,1,0,0,1,0,0,1,0,0,1,0,0,1,0,0,1,0,0,1,0,0,1,0,0,1,0,0,1,0,0,1,0,0,1,0,0,1,0,0,1,0,0,1,0,0,1,0,0,1,0,0,1,0,...]
2.2 Time-Based Localization

This section gives a detailed view of the localization technique on which this master thesis is built upon, called double differential time of arrival (DDDTOA). First, some well-known variations are presented, namely TDOA and TOA. These techniques are closely related to DDDTOA, and are therefore fit as an introduction.

2.2.1 Time Difference of Arrival

Normal TDOA uses the difference in time of arrival of a signal at two receivers, who are separated by some distance. The absolute time when the signal left the transmitter is not important, nor the time when the signal arrives at the two receivers. However, the synchronization between the receivers is vital for a correct calculation of the time difference. In practice, the signal to be located is recorded at both receivers. Then, the two versions are compared with each other to find the time delay [Arbring and Hedström, 2010]. The received signals can be described in the following way:

\[ x_1(t) = s(t) + w_1(t) \]
\[ x_2(t) = s(t + \Delta) + w_2(t) \]

\( x_1 \) is the signal recorded at receiver 1 and \( x_2 \) the same signal recorded at receiver 2 with some delay \( \Delta \). \( w_1 \) and \( w_2 \) represent additive white Gaussian noise (AWGN). Since the signals are recorded simultaneously, and the receivers being (to some extent) fully synchronized, \( \Delta \) can be determined by calculating the cross-correlation function \( r_{x_1x_2} \).

\[ r_{x_1x_2}(\tau) = E[x_1(t)x_2(t + \tau)] \] (2.1)

\( \Delta \) is determined as the \( \tau \) that maximizes the absolute value of the correlation function. The calculations can also be done in the frequency domain, and in this case \( \Delta \) is found as the gradient of the angle part of the cross spectra \( S_{x_1x_2}(f) = \mathcal{F}\{r_{x_1x_2}(\tau)\} \).

The time difference \( \Delta \) is then used together with the constant propagation speed of radio signals to calculate a hyperbola of possible positions for the origin of the signal.

\[ |\mathbf{P}_{MS} - \mathbf{P}_{RX1}| - |\mathbf{P}_{MS} - \mathbf{P}_{RX2}| = c\Delta \] (2.2)

\( \mathbf{P}_{RX1}, \mathbf{P}_{RX2} \) and \( \mathbf{P}_{MS} \) represent the positions in Cartesian coordinates of receiver 1, receiver 2 and the mobile, and \( c \) the speed of light. Figure 2.5 shows some examples of hyperbolas for different \( \Delta \). The receivers are represented by the large dots in the figure. To get an exact location of the transmitter, at least one more
2.2 Time-Based Localization

**Figure 2.5:** The possible locations (one hyperbola) for the transmitter, for a number of different values of the time delay $\Delta$. A smaller value of $\Delta$ gives a hyperbola closer to the midpoint between the two receivers.

receiver is needed in order to calculate an intersection point. The position of the receivers is important in order to get good accuracy, but also to avoid false mirror locations as could appear if the receivers are located on a line.

### 2.2.2 Time of Arrival

TOA\(^1\) is a technique that, as the name implies, uses the time instant for which the signal arrives at the receiver [Gezici et al., 2005]. In this case, synchronization as well as communication between the receiver and the transmitter is crucial.

The time ($\Delta$) it takes for the signal to travel from transmitter to receiver, again together with the speed of light, gives the radius ($\rho$) for a circle of possible locations of the source. Information about when the signal was sent is required in order to get the propagation time (this is the necessary communication between transmitter and receiver). Three or more calculations from different receivers determines the exact position, through regular triangulation. See Figure 2.6.

$$\rho = c\Delta \quad (2.3)$$

\(^1\)In this case, TOA is refered to both the name of the method, as well as the time of arrival for a signal.
TOA is a technique that can not be used in an electronic warfare situation (in terms of finding enemy forces), due to the fact that communication and synchronization between receiver and transmitter is needed. However, it is possible to calculate the position of the transmitter without the knowledge of when the signal was sent. By comparing the TOA values at the three receivers, the location of the transmitter can be found by solving an optimization problem; in contrary to calculating the intersection point of the three circles. This is known as differential TOA (DTOA).

### 2.2.3 Double Differential Time of Arrival

The technique presented and examined in this master thesis is called double differential time of arrival (DDTOA). The idea with this method is to determine the time delay $\Delta$ between two receivers, just like in TDOA but without the need for synchronization. The synchronization is instead done using a reference signal, where the origin of the signal is known. Also, instead of correlating the received signals, the time delays are calculated using the difference between the time of arrival values, as in DTOA.

Two signals are recorded at the receivers, one from the transmitter to be located, and one from the reference source.

In DDTOA, the *double* represents the added reference signal examined at each receiver to compensate for time synchronization errors. The *differential* stands for the difference between two time of arrival values of the same signal at two receivers, unlike normal TDOA which compare the signal recorded at two receivers (Equation 2.1).

The calculations to determine the actual position will be the same as for normal TDOA, it is the method of finding the time difference $\Delta$ that differs. Hence, the reason for only presenting a method to find one hyperbola, on which the user is located, in this thesis. The rest of the positioning is pure geometry and nothing new.
2.2 Time-Based Localization

2.2.3.1 Calculating the Time Difference

The system setup is again shown in Figure 2.7. $P_{RX1}$, $P_{RX2}$, $P_{MS}$ and $P_{BS}$ represent the positions of receiver 1 and 2, the mobile to be located and the reference source (base station). The time difference is given as

$$\Delta = \hat{\tau}_{MS,RX1} - \hat{\tau}_{MS,RX2} + \delta - (\hat{\tau}_{BS,RX1} - \hat{\tau}_{BS,RX2})$$  \hspace{1cm} (2.4)

where $\hat{\tau}_{X,Y}$ is the time of arrival at location $Y$ for a signal sent from location $X$. $\delta$ is the true time difference for a signal traveling from the reference source to receiver 1 and 2 respectively. As mentioned in Chapter 1, the positions of receiver 1, 2 and the reference source are known beforehand, so $\delta$ can be determined by geometry calculations.

The righthand side of equation 2.4 can be divided into two parts:

$$\left(\frac{\hat{\tau}_{MS,RX1} - \hat{\tau}_{MS,RX2}}{\text{Time diff. part}}\right) + \left(\frac{\delta - (\hat{\tau}_{BS,RX1} - \hat{\tau}_{BS,RX2})}{\text{Synchronization part (error)}}\right)$$

In the case where the receivers are synchronized, the reference source and thereby the synchronization part would not be required. This corresponds to

$$\delta - (\hat{\tau}_{BS,RX1} - \hat{\tau}_{BS,RX2}) = 0$$  \hspace{1cm} (2.5)

which of course goes hand in hand with the fact that the calculated reference time difference should be equal to the predetermined value $\delta$, according to

$$\hat{\tau}_{BS,RX1} - \hat{\tau}_{BS,RX2} = \delta$$  \hspace{1cm} (2.6)
Equation 2.6 will be used in the field experiment as a verification on how accurate the measurements are, by using synchronized receivers.

In the aspect of keeping a low profile in war, the communication between friendly forces must be kept to a minimum. Therefore, the terms in Equation 2.4 are reordered according to

$$\Delta = (\hat{\tau}_{MS,Rx1} - \hat{\tau}_{BS,Rx1}) - (\hat{\tau}_{MS,Rx2} - \hat{\tau}_{BS,Rx2}) + \delta$$

(2.7)

In this way, it is possible to subtract the time stamps at a specific receiver before sending the values to a third party for the $\Delta$-calculation. This comes in handy when averaging over a larger number of signals for one time difference calculation. An illustrative picture is shown in Figure 2.8.

**Figure 2.8:** Example of time stamps. The numbers are given in time units. According to Equation 2.4, the time difference will be $\Delta = (22 - 29) + (-3) - (8 - 6) = -7 - 3 - 2 = -12$. The sign of $\Delta$ and $\delta$ is determined by Rx2 subtracted from Rx1.

### 2.2.3.2 Evaluation of Bound for Synchronization Error

As mentioned in Section 2.1.5, it is the training sequences within the burst that will be used for the time stamps. They are sent with some time period $T_p$ separated from each other. $T_p$ is approximately 4.6 ms for the uplink communication, and approximately 46.2 ms for downlink communication. To be sure that the time stamps from the same transmitted training sequence are being compared, the synchronization error $\epsilon_{\text{SYNC}}$ needs to be below a certain limit.
2.2 Time-Based Localization

To start with, let's assume that

$$\Delta \ll T_p \quad \text{and} \quad \delta \ll T_p$$

This is a reasonable assumption, since the lower value on $T_p$, 4.6 ms, corresponds to a propagation distance of 1380 km for a radio signal. This is a distance much larger than that possible for mobile communication. Using this assumption, the synchronization error will be bounded by

$$|\epsilon_{\text{SYNC}}| < \frac{T_p}{2}$$

Figure 2.9 shows the area for which the synchronization error can drift, without the possibility of comparing two different training sequences.

In the case when the synchronization error is bigger than half the training sequence repetition period, some kind of extra information about the training sequence is required. This is where the TDMA frame number (FN) can be used. The data part of an SCH burst contains a number specific for the TDMA frame which the burst belongs to. This makes it possible to attach a number to each SCH training sequence, and in this way make sure that the same training sequence is used for the time stamp at both receivers, regardless of how large the synchronization error is.

To make sure that the same training sequences are used for the uplink communication, the synchronization error is first calculated and then compensated for. After this, it is possible to pair two matching uplink training sequences and calculate the time difference $\Delta$. In this case, the advantage gained from Equation 2.7 is lost, since both TOA values need to be sent to the third party instead of only the difference between the values.
This chapter describes the method used to implement the theory from Section 2.2.

### 3.1 Correlation

To determine the time stamps for which the signals arrives at the receivers, correlation is used. How good two signals correlate with each other can be seen as a measurement on how closely related they are to each other. The recorded signals are therefore correlated with the known training sequences. The highest values (i.e. the peaks) in this correlation function should thereby point out where the received training sequences are located within the recorded signals. The time stamps for these peak values are then used as the time of arrival for the signal. See Figure 3.1 and 3.2.

![Diagram of Cross Correlation and Peak Detection](image)

**Figure 3.1:** Cross correlation between the received signal and the known training sequence, together with peak detection, gives the time of arrival value.
3.1.1 Mathematical Description

To get a better understanding of why this works, we use the squared Euclidean distance between two signals [Larsson, 2012], for example $y_1(t)$ and $y_2(t)$. The Euclidean distance is zero only if $y_1(t) = y_2(t)$ for all $t$. Hence, the shorter the squared Euclidean distance is, the more similar the signals are.

A simple model of the system is

$$x(t) = s(t - \tau) + w(t)$$

where $x(t)$ is the received signal which is described as a time delayed version of the sent signal $s(t)$ with some added noise $w(t)$. Determine time of arrival will correspond to finding the time delay, if the receiver knows the time the signal was sent. Note that this is only true if transmitter and receiver are synchronized, which they are not in this case. However, the actual propagation time delay is not of interest here, only the differential time delay between two receivers.

Without the influence of noise, $x(t)$ and $s(t - \tau)$ would be equal, and the squared Euclidean distance zero. Thus, minimizing the squared Euclidean distance between $x(t)$ and $s(t - \tau)$ should give the best approximation of the time delay. This can be mathematically described as

\footnote{With some restrictions on the signals}
\[ \int_{-\infty}^{\infty} (x(t) - s(t - \tau))^2 \, dt = \int_{-\infty}^{\infty} (x^2(t) + s^2(t - \tau) - 2x(t)s(t - \tau)) \, dt = \int_{-\infty}^{\infty} x^2(t) \, dt + \int_{-\infty}^{\infty} s^2(t - \tau) \, dt - 2 \int_{-\infty}^{\infty} x(t)s(t - \tau) \, dt \] (3.1)

In this way it is possible to see that minimizing the squared Euclidean distance is the same as maximizing the expression

\[ r_{x,s}(\tau) = \int_{-\infty}^{\infty} x(t)s(t - \tau) \, dt \]

with respect to the time delay \( \tau \). We now formulate the formal definition of (deterministic) cross correlation between two, possibly complex, signals:

\[ r_{y_1y_2}(\tau) = \int_{-\infty}^{\infty} y_1^*(t)y_2(t + \tau) \, dt \]

where \(< * >\) denotes complex conjugate.

The \( \tau \)-value which gives the highest value of \( |r_{x,s}(\tau)| \) will be the estimated time of arrival \( (\hat{\tau}) \) for the training sequence.

To summarize, the received signal is correlated with the known training sequence. The parts in the received signal where the training sequence is located should give the highest values for the correlation function, according to Equation 3.1 (they are likely most similar, so the euclidean distance is minimized). The time stamp for these peak values are used as the time of arrivals. In this way, it is possible for two receivers to compare time of arrivals of the same transmitted training sequence. The added noise can be seen as a way of distorting the peaks.

In reality, there exists no infinitely long signals. The practical aspects of implementing the correlation function will be given later in this chapter.
3.1.2 Comments on Accuracy

How accurate the calculation of the time stamp can be, comes down to essentially three different things: how high the signal to noise ratio (SNR) is, how long the overlapping correlation sequence is (meaning, the length of the training sequence, $L$) and also how much bandwidth ($B$) the transmitted signal occupies? The first thing is easy to get a grip on. The higher the noise levels are, the more affected by the noise will the received training sequence be. This will influence the similarity between the received training sequence and the real one that is used for correlation, and there by the sharpness of the peak. If the noise is too high, it could even be impossible to distinguish the peak from the rest of the correlated data.

The reaction on the peak due to longer or shorter training sequences is also quite intuitive. The more unique information you have available, the more reliable will the outcome be, whatever it is. A longer training sequence should therefore give a better estimation of the time of arrival. As seen in Chapter 2, the two available types of training sequences are 26 respectively 64 bits long. In mobile communication, these are used for detection and demodulation, as a way of estimating the channel. The shorter one is used in a burst whose main purpose is to transmit data, while the longer one is used in a burst for synchronization. There is of course always a trade-off between good channel estimation and high data throughput. The 64 bits sequence will be used for the signals sent from the base station since these bursts are broadcast. The 26 bits sequence will be used for the signals transmitted from the mobile station. Hence, the accuracy of the TOA from the base station should be better than the one from the mobile. It should also be noted that the training sequences are designed to have good auto correlation properties, i.e. high peaks.

The connection between available bandwidth and the sharpness of the correlation peak is perhaps not as intuitive. Approximately, the width of the peak is inversely proportional to the bandwidth of the signal [Larsson, 2012]. This is due to the uncertainty principle of the Fourier transform. The idea of this principle states that is impossible for a signal to have all its energy within a certain time interval, and at the same time only occupy a limited number of frequencies [Du]. One way to exemplify this is to consider the Fourier transform of the sinc function, which is a rectangular function:

$$y(t) = \text{sinc}(at) \rightarrow \mathcal{F}\{y(t)\} = \begin{cases} 1/a & \text{if } |f| \leq a/2 \\ 0 & \text{if } |f| > a/2 \end{cases}$$

A higher value of $a$ provides a more narrow peak in the time domain, but a wider box in the frequency domain. This implies that the more bandwidth you have available, the more accurate will the calculation of the time of arrival be. Also, the energy should be spread out as evenly as possible over the bandwidth. A measure of this is known as the effective bandwidth.
$L$ and $B$ are predefined values of the GSM standard, and thereby constant in this case. The SNR is hard to influence, apart from choosing a good receiver position relative to the base station and using a good antenna high above the ground. However, there is one thing that can increase the accuracy of the calculations; namely the use of sample interpolation.

### 3.2 Curve Fitting

Sample interpolation, or curve fitting, is a method which estimates a larger number of function values given a smaller, discrete set of values. In this case, the correlation peaks will be approximated by a polynomial of the second order. Instead of only letting the maximum value of the peak represent the position for the time of arrival, several neighbouring samples are interpolated to a second degree curve. The zero-root of the derivative of this curve is then used as the time stamp. See Figure 3.3.

### 3.3 Averaging

Since one single phone call includes a large number of training sequences ($M$), it is possible to decrease the estimation error by averaging over several TOA measurements. This gives

$$\Delta = \frac{1}{M} \sum_{i=1}^{M} (\hat{\tau}_{MS,RX1}[i] - \hat{\tau}_{MS,RX2}[i] + \delta - (\hat{\tau}_{BS,RX1}[i] - \hat{\tau}_{BS,RX2}[i]))$$

(3.3)

where $\hat{\tau}[i]$ is a vector containing $M$ different TOA values from one telephone call.

### 3.4 Implementation

All of the implementation has been done in MATLAB.

#### 3.4.1 Demodulation and Frequency Correction

Demodulating and decoding the downlink broadcast signals is a field big enough to be a master thesis of its own. It includes subjects as time synchronization, frequency correction, equalization, demodulating symbols into bits and decoding the raw data bits into readable information. Therefore, the theory behind this part is left out of this report. For the interested, [Pathak] and [Bapat et al., 2005] are suggested. Frequency correction is sometimes needed because of receiver hardware limitations (unstabilized oscillators).

The code used for the demodulation as well as the frequency correction in the implementation has been taken from [Ekstrøm and Mikkelsen, 1997].
Figure 3.3: The figure shows the function $y(t) = -t^2 + 2$, and '*' marks the available samples around the peak ($t = 0$). By only using the maximum value, the time of arrival would be -0.2. However, by interpolating the samples as a second degree curve, and calculate an estimate of the value $t$ where $y'(t) = 0$, the time of arrival will become approximately 0 (using MATLAB’s function polyfit).

### 3.4.2 Practical Aspects

When talking into a mobile phone, the amplitude of the signal goes up and down depending on when you are speaking and when you are silent between the words. Because of this, some graphical observations of the correlation plots were done, to chose the part of the signal with the highest amplitude.

### 3.4.3 Discrete Correlation

For the discrete implementation of the cross correlation function, MATLAB’s `xcorr` was used [Mathworks, 2013]. It estimates the true value as
\[ \tilde{r}_{y_1y_2}[n] = \begin{cases} 
\sum_{m=0}^{N-n-1} y_1[m+n]y_2^*[m] & \text{for } n = 0, ..., N-1 \\
\tilde{r}_{y_2y_1}^*[-n] & \text{for } n = -(N-1), ..., -1 
\end{cases} \]

where \( N \) is the number of samples for the longer signal (i.e. the received signal).

### 3.4.4 Interpolation

The interpolation was implemented using MATLAB’s function \texttt{polyfit}, and the calculation of the zero-root of the derivative by using \texttt{polyder} followed by \texttt{roots}.

### 3.4.5 Modulated Training Sequence

To get a better understanding of how to implement the modulated baseband versions of the training sequences, a different expression for the frequency function \( g(t) \) was derived.

The frequency function \( g(t) \) can be approximated as a Gaussian distribution according to

\[ g(t) = h(t) \ast \text{rect} \left( \frac{t}{T} \right) \]

\[ = \frac{1}{\sqrt{2\pi\sigma T}} \int_{-\infty}^{\infty} \exp \left( -\frac{-\tau^2}{2(\sigma T)^2} \right) \text{rect} \left( \frac{t - \tau}{T} \right) d\tau \]

\[ = \left| -\frac{T}{2} \leq t - \tau \leq \frac{T}{2} \Rightarrow \tau \geq t - \frac{T}{2} \text{ and } \tau \leq t + \frac{T}{2} \right| \]

\[ = \frac{1}{T} \frac{1}{\sqrt{2\pi\sigma T}} \int_{t-T/2}^{t+T/2} \exp \left( -\frac{-\tau^2}{2(\sigma T)^2} \right) d\tau \]

\[ = \frac{1}{T} \frac{1}{\sqrt{2\pi\sigma T}} \left( \int_{t-T/2}^{\infty} \exp \left( -\frac{-\tau^2}{2(\sigma T)^2} \right) d\tau - \int_{t+T/2}^{\infty} \exp \left( -\frac{-\tau^2}{2(\sigma T)^2} \right) d\tau \right) \]

\[ = \frac{1}{T} \left( Q \left( \frac{t-T/2}{\sigma T} \right) - Q \left( \frac{t+T/2}{\sigma T} \right) \right) \]

\[ \approx \frac{1}{T} \left( T \frac{1}{\sqrt{2\pi\sigma_2}} \exp \left( \frac{-t^2}{2\sigma_2^2} \right) \right) = \frac{1}{\sqrt{2\pi\sigma_2}} \exp \left( \frac{-t^2}{2\sigma_2^2} \right) \]

Note that the last row in the expression is only an approximation, where \( \sigma_2 = 1.957002 \cdot 10^{-6} \). This gives the following appearance of the phase function \( \varphi(t) \):
\[ \varphi(t) = \sum_i \alpha_i \mu_i \pi \int_{-\infty}^{t-iT} \frac{1}{\sqrt{2\pi\sigma_2^2}} \exp\left(-\frac{\tau^2}{2\sigma_2^2}\right) d\tau \]

(3.5)

\[ = \sum_i \alpha_i \mu_i \pi \left( \int_{-\infty}^{\infty} \frac{1}{\sqrt{2\pi\sigma_2^2}} \exp\left(-\frac{\tau^2}{2\sigma_2^2}\right) d\tau - \int_{t-iT}^{\infty} \frac{1}{\sqrt{2\pi\sigma_2^2}} \exp\left(-\frac{\tau^2}{2\sigma_2^2}\right) d\tau \right) \]

\[ = \sum_i \alpha_i \mu_i \pi \left( 1 - Q\left( \frac{t-iT}{\sigma_2} \right) \right) \]

To get the discrete values of the phase function, \( \varphi(t) \) is sampled for \( t = nT \), with some possible oversampling:

\[ \varphi[n] = \varphi(t = \frac{nT}{\Lambda}) \quad \text{for} \quad n = 1, 2, 3, ..., L \cdot \Lambda \]  

(3.6)

where \( L \) is the number of modulated symbols and \( \Lambda \) the oversampling rate. The baseband representation of the modulated training sequence can then be implemented as

\[ x_{TR}[n] = e^{j\varphi[n]} \]  

(3.7)

### 3.4.6 Algorithms

Figures 3.4 - 3.7 show block diagrams over the implementation algorithms, in correct sequence of execution order. They give a rough description on the different steps and the input and output parameters.

**Figure 3.4:** The received downlink signal is first demodulated to retrieve the frequency offset \( f_{\text{offset}} \), the BCC and the FN. Finding the frequency offset is seen as a part of the demodulation process.
Figure 3.5: Modulation of the training sequences. Input is bits and output is the complex baseband representation. BCC is used when modulating the 26 bit sequence (uplink).

Figure 3.6: Block diagram showing the algorithm to find the TOA for the received signal. The process is iterated over the number of available correlation peaks ($M$) in the signal. FN is used for the downlink signal, to pin a specific number to the TOA value.

Figure 3.7: Block diagram showing the calculations of $\Delta$, given the true time delay $\delta$ and the TOA values as input. The result is averaged over the available number of peaks ($M$).
Simulations were done in order to test the method. It should be noted that the model used for the simulations is quite simple. It doesn’t say much about the real case, since difficulties like for example multipath propagation is avoided. Also, the available size of the bandwidth is neglected. However, it is a good way of testing the correlation and interpolation, with respect to SNR and the length of the training sequence.

4.1 System Model

The positions for the nodes in the simulation model can be seen in Figure 4.1. The imaginary receivers, base station and mobile station are placed in the corners of a square. Hence, both $\Delta$ and $\delta$ are equal to zero.

The signals used in the model are the modulated baseband version of the known training sequences, together with the imaginary received signal created as the training sequence with added white gaussian noise.

$$x_{TR}[n]$$  
$$\tilde{x}[n] = x_{TR}[n] + w[n]$$

4.2 Calculations

The idea is to first get an estimation of the error of the TOA values by correlating the modulated training sequence with the noisy version, determine the location of the peak value by interpolation, and finally comparing it with the expected
value zero. See Figure 4.2. Correlation between the two signals without adding noise gives the auto correlation function for the training sequence, which in theory is symmetric around zero. Hence, comparing the TOA estimate with respect to the zero value shows how the peak detection is influenced by the noise.

The TOA error, $\hat{\tau}_{\text{ERROR}}$, is then used to calculate the root mean square error (RMS) of the estimation, according to

$$
\tilde{\epsilon}_{\text{TOA}} = \sqrt{\frac{1}{N_{\text{EST}}} \sum_{j=1}^{N_{\text{EST}}} (\hat{\tau}_{\text{ERROR}}[j])^2}
$$

(4.1)

$N_{\text{EST}} = 1000$ is the number of estimated TOA errors. By doing this for a number of different values on the noise energy and for both training sequences, it is possible to compare RMS with respect to SNR and signal length.

The RMS values from the TOA estimation are then used in Equation 3.3 to get a relationship between SNR and the RMS for the time delay $\Delta$. A single value of the DDTOA error, $\Delta_{\text{ERROR}}$, is estimated as

Figure 4.1: The hypothetical locations in the simulation model. Both $\Delta$ and $\delta$ are equal to zero due to the symmetry between the four nodes.

Figure 4.2: Correlation between the two signals used in the model, followed by peak detection gives the error of the TOA estimate.
\[ \Delta_{\text{ERROR}} = \frac{1}{M} \sum_{i=1}^{M} \left( \chi_{UL}[i] - \xi_{UL}[i] - (\chi_{DL}[i] - \xi_{DL}[i]) \right) \] (4.2)

where the TOA values are implemented as normally distributed variables with zero mean and a standard deviation equal to the RMS from the TOA estimation:

\[ \chi_{UL}, \xi_{UL} \sim N(0, \tilde{\epsilon}_{\text{TOA,UL}}) \]
\[ \chi_{DL}, \xi_{DL} \sim N(0, \tilde{\epsilon}_{\text{TOA,DL}}) \]

The subscripts UL and DL indicates downlink and uplink communication. Equation 4.2 gives an estimation of the DDTOA error since the true values of \( \Delta \) and \( \delta \) in the model are both equal to zero. The RMS of the DDTOA estimation can finally be calculated according to

\[ \tilde{\epsilon}_{\text{DDTOA}} = \sqrt{\frac{1}{N_{\text{EST}}} \sum_{j=1}^{N_{\text{EST}}} (\Delta_{\text{ERROR}}[j])^2} \] (4.3)

### 4.3 Results

First, the RMS value for a TOA estimation were calculated without adding any noise, to see that the location of the peak actually is zero. This gives

\[ \tilde{\epsilon}_{\text{TOA}} = 2.245 \cdot 10^{-22} \text{ s} \]

which in this case very well can be approximated with zero. The sampling frequency, i.e. the inverse of the time between two samples, used in the model is the same as in the laboratory trials and is equal to 4'333'328 Hz (the symbol rate oversampled by 16).

Figures 4.3 and 4.4a show the correlation functions for the 64 bit and the 26 bit training sequences respectively, while Figure 4.4b shows a zoomed in version of 4.4a. In the latter, it is possible to see how the noise affects the location of the correlation peak.
**Figure 4.3:** Plot of the (normalized) correlation function for the 64 bit training sequence, without noise. The function is symmetric around zero.
4.3 Results

Figure 4.4: (a) Plot of the (normalized) correlation function for the 26 bit training sequence (BCC = 1). Both without the impact of noise and with added noise (SNR = -5 dB). (b) Zoom in on the correlation function. The peak is located some what to the right of the zero value, due to the influence of the noise.
The RMS from the TOA estimations can be found in Figure 4.5. The figure clearly shows how the error decreases as the SNR increases, and also that the longer training sequence gives better results than the shorter one. All according to the argumentation on accuracy in Chapter 3.

Figure 4.6 shows the result of the DDTOA estimation. This time, the RMS is multiplied by \( c \) to get the error in meters instead of seconds. Simulations where done using different values on \( M \) for the averaging. The plot shows that averaging can be very useful when the SNR is low, but of less importance when the SNR is high.

The RMS value connected to a specific SNR in Figure 4.5 were used in the calculation of the RMS value in Figure 4.6, connected to the same SNR.

It should be noted that the error values presented here are not the distance error from the actual mobile station position, but the error from one \( \Delta \) calculation between two receivers, at the baseline (the line intersecting with both receivers).

\[\text{Figure 4.5: Plot showing the RMS due to the impact of noise.}\]
Figure 4.6: The RMS for the estimation of $\Delta$, when averaging over 1, 10 and 100 of each TOA value.
This chapter describes the trials that have been done to examine the DDTOA system, along with their results. Experiments were made in both a laboratory and in a field test. In the laboratory, the two receivers Rx1 and Rx2 were connected to the same antenna, meaning, the receivers are located at the same position. No localization of the mobile signal is possible in this case, since the time delay $\Delta$ always will be zero, no matter where the mobile station is located. However, it is possible to test the implementation and the accuracy of the calculations. Since both $\Delta$ and $\delta$ is zero in this case, you can calculate the time delay for a phone call, compensate for the synchronization error with the help from a reference signal and then compare it to the zero value. This provide an indication of the error margin for the system.

For the field experiment, one of the receivers was put in a car and driven away from the laboratory. This setup made it possible to test the system in an actual positioning situation.

First, the equipment is described, then the system setups and finally the results of the trials.

### 5.1 Receiver Hardware

A block diagram of the receiver can be seen in Figure 5.1. In short, it is made of an antenna, a tuner, an A/D-converter, a DDC (digital down converter) and a storage system. The tuner moves the RF (radio frequency) signal from the 900 MHz band down to an IF (intermediate frequency) signal centered around 10.7 MHz. The A/D-converter together with the DDC converts the analog signal to a digital baseband signal (I/Q data) and stores it on a file. The DDC has multiple
inputs making it possible to record the signal from the mobile and the signal from the base station at the same time.

5.2 TEMS Mobile Phone

In order to simplify the experiments, a special kind of mobile phone was used. It has an operation mode called TEMS (test mobile system), which makes it possible to choose between GSM and 3G, see the available frequency cells (channels) and also to force the mobile to transmit and receive on a particular channel. In this way, the receivers can tune in on the correct frequency from the beginning, instead of searching through the entire frequency band. Since these trials are not made in real time, searching for the mobile signal is not even an option. Further, one can be sure that it is the signal from the correct mobile that is being localized. If more than one mobile should use the same frequency channel, it will be noticed since more than one time slot will be occupied.

5.3 Execution

A phone call made from the TEMS mobile was recorded using the receivers. The recording time was set to 6 s (longer recording time is possible but creates problems with large data files). The downlink frequency $F_d$ was set to 952.4 MHz, corresponding to channel 87. The analog signal is sampled with a frequency of 160 MHz. After the signal processing in the DDC, the signal is downsampled to 5 MHz, to extract unnecessary information and reduce the size of the file. Finally, the digital signals are reshaped in MATLAB to a sample frequency $F_s = 4\,333\,328$ Hz, to match an oversampling of the symbol rate by 16 (for simplicity, the oversampling should be a multiple of 4, since the guard periods in the bursts have a duration of 8.25 bits).

To induce a synchronization error within the system, one receiver (Rx1) was running with a GPS clock reference, while the other (Rx2) used a floating clock reference. This setup created a synchronization error between 0 and 1 s. A detailed block diagram of the links and wires can be found in Figure 5.2. Two EB200...
Figure 5.2: A detailed view of how the components in the receivers are connected, in the case for the laboratory trials. For the field experiment, the setup was the same, except for the receivers having their own antenna. The tuners, as well as the 160 MHz signal generator, uses a 10 MHz clock reference as a stabilizer. The 1 PPS (pulse per second) is used to trigger the recording. Since Rx1 uses a GPS as reference while Rx2 uses a floating reference, the recordings are triggered at different times within the same second, creating a synchronization error between 0 and 1 s.
tuners were used together with each receiver; one tuned in on the downlink frequency and the other on the uplink frequency.

Some attempts were also made using a GPS reference in both receivers, to see if there would be any difference in the performance.

### 5.3.1 Laboratory Setup

For the laboratory trials, the two receivers were connected to the same antenna, which was placed on the roof of the building. Figure 5.3 shows the positions for the four objects. Two different locations were tested for the mobile, one close to the antenna (to provide better SNR) and one further away.

![Diagram](image.png)

**Figure 5.3:** Positions for the laboratory trials. A and B marks the spots for the mobile stations. The antenna connected to the two receivers is located on the roof of the laboratory. The area is located south of Linköping University, Linköping, Sweden.

As mentioned before, the true values on $\Delta$ and $\delta$ in this case are both zero. Table
Table 5.1: Parameters for the laboratory attempts. $F_u$ is the uplink frequency.

<table>
<thead>
<tr>
<th>Attempt</th>
<th>Position</th>
<th>$F_u$ [MHz]</th>
<th>BCC</th>
</tr>
</thead>
<tbody>
<tr>
<td>I</td>
<td>B</td>
<td>907.4</td>
<td>1</td>
</tr>
<tr>
<td>II</td>
<td>B</td>
<td>913</td>
<td>5</td>
</tr>
<tr>
<td>III</td>
<td>A</td>
<td>907.4</td>
<td>1</td>
</tr>
</tbody>
</table>

5.1 shows the parameters for the attempts using the laboratory setup.

5.3.2 Field Test Setup

Figure 5.4 shows the positions for the field test. The location for the mobile station was chosen to give approximately the same distance to both receivers, and in this way provide equal signal strength at both receivers. The true values on $\Delta$ and $\delta$ was determined using the GPS coordinates for the objects, converting them to RT90 (Rikets nät or Swedish grid) coordinates followed by geometrical calculations of the distances between the objects. Rx2 had a large bias due to a long cable between the antenna and the tuner. However, this bias is the same for $\Delta$ and $\delta$, so it will not effect the result.

Table 5.2 below gives the parameters for the attempts in the field test.

Table 5.2: Parameters for the attempts in the field experiments.

<table>
<thead>
<tr>
<th>Attempt</th>
<th>$F_u$ [MHz]</th>
<th>BCC</th>
</tr>
</thead>
<tbody>
<tr>
<td>IV</td>
<td>909.4</td>
<td>7</td>
</tr>
<tr>
<td>V</td>
<td>909.4</td>
<td>7</td>
</tr>
<tr>
<td>VI</td>
<td>909.4</td>
<td>7</td>
</tr>
<tr>
<td>VII</td>
<td>909.4</td>
<td>7</td>
</tr>
<tr>
<td>VIII</td>
<td>907.4</td>
<td>1</td>
</tr>
<tr>
<td>IX</td>
<td>907.4</td>
<td>1</td>
</tr>
</tbody>
</table>
Figure 5.4: Positions for the field experiment. The position for the mobile station (MS) is approximately the same as the one used for the laboratory trials (B).
5.4 Results

5.4.1 Received Signals

First, two examples of received signals are shown to illustrate the difference between the laboratory results and the field experiment results. Figure 5.5 shows the received uplink signals from Attempt I. In this case, the recorded signals look the same in terms of amplitude variations. It is possible to get a rough estimation of the synchronization error just by looking at the plot.

Figure 5.6 shows the received uplink signals from Attempt IV. The signal recorded at RX1 is a little bit stronger than the one recorded at RX2, and the amplitude variations are not the same.

5.4.2 Laboratory Trials

The results of the calculation of $\Delta_{\text{ERROR}}$ from Attempt I, II and III can be seen in Figures 5.7, 5.8 and 5.9. The results are given in meters after multiplying the time delay with the speed of light. The histograms show how the values of $\Delta_{\text{ERROR}}$ are distributed. All attempts gave quite good results, as the figures show. The three distributions are centered around zero, with most of the values close to the true value and a few less accurate. The sign of the error is determined by RX2 subtracted from RX1.

The outcome after averaging can be found in Table 5.3. When calculating the mean value of $\Delta_{\text{ERROR}}$, the error is below 1 m in all three attempts.

Figures 5.10 and 5.11 shows the calculated differences between the TOA values, for downlink and uplink respectively. In these plots, it is possible to see how the synchronization error drift in time due to the floating time reference. They also show that the accuracy from the downlink signal seems somewhat better than that of the uplink signal. Finally, both signals indicates the same synchronization error, as they should since both $\Delta$ and $\delta$ are zero.

<table>
<thead>
<tr>
<th>Attempt</th>
<th>$M$ (Uplink)</th>
<th>$M$ (Downlink)</th>
<th>$\Delta_{\text{ERROR}}$ [m]</th>
<th>Synchronization</th>
</tr>
</thead>
<tbody>
<tr>
<td>I</td>
<td>169</td>
<td>100</td>
<td>-0.77</td>
<td>No</td>
</tr>
<tr>
<td>II</td>
<td>75</td>
<td>74</td>
<td>+0.78</td>
<td>No</td>
</tr>
<tr>
<td>III</td>
<td>1000</td>
<td>120</td>
<td>-0.94</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Table 5.3: Results from the laboratory trials. $M$ is the number of peaks used for TOA calculations during the call (the number used for averaging).
**Figure 5.5:** Absolute value of the received uplink signals from Attempt $i$. The upper signal is from receiver 1, and the lower from receiver 2. It is possible to see how the amplitude variates in time. Due to this, only the part from approximately 3 - 4.5 s were used to calculate the TOA values. Compare with Figure 5.10.

**Figure 5.6:** Absolute value of the received uplink signals from Attempt IV. The upper signal is from receiver 1, and the lower from receiver 2.
Figure 5.7: Histogram over the $\Delta_{\text{ERROR}}$ values for Attempt I. The values of $\Delta_{\text{ERROR}}$ are multiplied by $c$ to get the results in meters. The mean value is $-0.77$ m after averaging. The correct value is zero (no error).

Figure 5.8: Histogram over the $\Delta_{\text{ERROR}}$ values for Attempt II. The mean value is $0.78$ m.
Figure 5.9: Histogram over the $\Delta_{\text{ERROR}}$ values for Attempt III. The mean value is -0.94 m.

Figure 5.10: The TOA differences for Attempt I. The uplink signal is the signal from the mobile, and the downlink signal is the signal from the base station. As can be seen in the figure, the synchronization error drift in time. Due to this fact, the synchronization error was interpolated as a first order polynomial, instead of the normal averaging.
5.4 Results

Figure 5.11: The TOA differences for Attempt II.

5.4.3 Field Test

The results of the calculation of $\Delta$ from the field experiments can be found in Figures 5.13-5.18, in the end of this chapter. The results are given in meters after multiplying the time delay with the speed of light. These figures also show how the values of $\Delta$ are distributed during one phone call (attempt). The true value of $\Delta$ was calculated to -59 m ($R_{x1} - R_{x2}$). Table 5.4 shows the outcome after averaging.

Table 5.4: Results from the field experiments. The number of training sequences ($M$) used in one attempt depends on the appearance of the signal; only the parts with high amplitude (relative the noise) were used.

<table>
<thead>
<tr>
<th>Attempt</th>
<th>$M$ (Uplink)</th>
<th>$M$ (Downlink)</th>
<th>$\Delta$ [m]</th>
<th>$\Delta_{\text{error}}$ [m]</th>
<th>Synchronization</th>
</tr>
</thead>
<tbody>
<tr>
<td>IV</td>
<td>650</td>
<td>93</td>
<td>-70</td>
<td>-11</td>
<td>No</td>
</tr>
<tr>
<td>V</td>
<td>620</td>
<td>117</td>
<td>-140</td>
<td>-81</td>
<td>No</td>
</tr>
<tr>
<td>VI</td>
<td>525</td>
<td>120</td>
<td>-169</td>
<td>-110</td>
<td>Yes</td>
</tr>
<tr>
<td>VII</td>
<td>75</td>
<td>120</td>
<td>-100</td>
<td>-41</td>
<td>Yes</td>
</tr>
<tr>
<td>VIII</td>
<td>200</td>
<td>110</td>
<td>-256</td>
<td>-197</td>
<td>No</td>
</tr>
<tr>
<td>IX</td>
<td>125</td>
<td>110</td>
<td>-120</td>
<td>-61</td>
<td>No</td>
</tr>
</tbody>
</table>
Figure 5.12: The $\Delta$ values from Attempt V. The values seem to oscillate outside the variation in accuracy. The part used for the calculations is about 3 s long.

5.4.4 Comments on Results

There is a lot of things that can be said about the results from the laboratory trials and the field test. Yet, it is hard to draw any good conclusions from the outcome. To start with, the results from the trials that were made in the laboratory are quite good; all of the attempts have an error below 1 meter. This is perhaps even better than expected, given the available bandwidth that GSM signals provide and the comments on accuracy from Section 3.1.2. However, there are single error values that are larger than 200 m. Without the averaging over several $\Delta$-calculations from the same phone call, the result would in most cases be poor.

On the other hand, the outcome of the field experiments was not as good. By looking at the histograms from Attempt IV-IX, the error distribution seems to be quite similar to that of Attempt II (ranging from about -150 m to +150 m), but unfortunately not centered around the correct value. This could have been explained by a bias in the calculations or in the equipment setup, if it wasn’t for the fact that the bias differs from one attempt to another. It was also noted during the calculations that the result differs within one attempt depending on which part of the signal that was used\(^1\).

Figure 5.12 shows an example of how the $\Delta$ values oscillates during one phone call. The values are from Attempt V.

What this floating bias depends on is hard to say. The first thing that comes to mind is multipath propagation, since it is one thing that clearly differs between

\(^1\)It should be noted that the results shown in the previous chapter are not chosen as the best ones. The part of the signal with the highest correlation peaks was always chosen for the calculations, no matter the outcome.
the laboratory trials and the field test. In the first case, since both receivers are connected to the same antenna, the effect of multiple paths is the same for both receivers. This means that the error caused by this phenomena will be avoided by the differential calculation of TOA values. In the latter case though, the radio waves from the mobile station can take different paths when traveling to the receivers. However, this error should be rather constant, but perhaps the small wavelengths and the strong winds (> 10 m/s) during the field test can cause these fluctuations.

**Figure 5.13**: Histogram over the Δ values from Attempt IV. The mean value is -70 m. The correct value is -59 m. The sum of the bars is the number of training sequences (M, uplink) used for averaging, in this case 650. Compare with Table 5.4.
Figure 5.14: Histogram over the $\Delta$ values from Attempt v. The mean value is -140 m.

Figure 5.15: Histogram over the $\Delta$ values from Attempt vi. The mean value is -169 m.
5.4 Results

Figure 5.16: Histogram over the $\Delta$ values from Attempt VII. The mean value is $-100$ m.

Figure 5.17: Histogram over the $\Delta$ values from Attempt VIII. The mean value is $-256$ m.
Figure 5.18: Histogram over the Δ values from Attempt IX. The mean value is -120 m.
This chapter summarizes the work and gives some suggestions on future work.

### 6.1 Results

The final conclusion of the results is that it will be difficult to locate the mobile station using the current state of the implementation. Still, there is some potential in the possibilities of averaging over large number of training sequences for a single calculation. More research needs to be done to find out what is causing the big errors, before anything concrete can be said about the accuracy of the method.

### 6.2 Suggested Improvements

The first step in the improvements would be to find out what causes the floating bias. To be able to do this, more efficient algorithms for analyzing the data should be developed. At this stage, it is too much manual work, giving long calculation times. This makes it hard to evaluate large amounts of data. Also, more robust equipment can be used, e.g. directional antennas. The location of the base station is always known, so it is possible to aim the antenna at its direction. This will improve the SNR. To overcome the problems due to multipath propagation, there are various methods of super-resolution techniques that could be worth looking into.
6.3 Future Developments

To further investigate in the possibilities of DDTOA, there are a lot of other signals of opportunity that can be used for synchronization. For example, radio AM-signals or wireless television signals. Another idea could be to create your own reference signal. In this way, it is possible to use long training sequences with good auto-correlation properties. The drawback of this method would be the need of an additional object in the system, and also the extra "unnatural" communication that can be detected by the opponent.

A variation of the method could be to only use the synchronization part of the equation, since the reference signals are generally stronger and easier to handle than those from the cell phone. When the synchronization error is found, it can be used together with the technique for normal TDOA.

6.4 Final Comments

During the field experiment, some additional positions were tested, further away from the receivers. The signals from these locations were in most cases very weak. A problem with the mobile phone is its power control. Since the reception to the base station is very good, the mobile lowers the power for transmitting, making it hard for the receivers to detect the signals (the base station uses much bigger antennas with more gain than the ones used in the field test). The idea from the beginning was to compare the stronger signals with the weaker, too see if there would be any difference in performance. However, since the outcome from the strong signals were poor, the result from the weak signals were only briefly examined and excluded from the report.

The starting point for this thesis was the problems with synchronizing receivers in a positioning system. Normal TDOA is dependent on GPS signals, so the idea was to create a system that could be used if the connection to the satellites is lost. In retrospect, the focus should perhaps have been more towards the synchronization part of this method, and less on the actual positioning. In this way, maybe the outcome would have been more satisfying.
List of Figures

1.1 Overview of the system. .............................................. 2

2.1 (a) An overview of the frame structure of GSM. (b) Every 0’th slot in each TDMA frame is put together to create one control channel (CCH) multiframe. \( F = \text{FCCH burst}, S = \text{SCH burst} \) and \( I = \text{Idle} \). ................................. 6

2.2 Structure of an FCCH burst. ........................................... 7

2.3 Structure of an SCH burst. ............................................. 8

2.4 Structure of a normal burst. .......................................... 8

2.5 The possible locations (one hyperbola) for the transmitter, for a number of different values of the time delay \( \Delta \). A smaller value of \( \Delta \) gives a hyperbola closer to the midpoint between the two receivers. ................................................................. 13

2.6 Positioning using TOA. The arrow marks the spot of the transmitter \( \text{Ms} \). ................................................................. 14

2.7 Overview of the system. .................................................. 15

2.8 Example of time stamps. The numbers are given in time units. According to Equation 2.4, the time difference will be \( \Delta = (22 - 29) + (-3) - (8 - 6) = -7 - 3 - 2 = -12 \). The sign of \( \Delta \) and \( \delta \) is determined by \( \text{RX2 subtracted from RX1} \). ......................... 16

2.9 Synchronization error. .................................................... 17

3.1 Cross correlation between the received signal and the known training sequence, together with peak detection, gives the time of arrival value. ............................................................... 19

3.2 Correlation peak gives the time of arrival value. .................. 20

3.3 The figure shows the function \( y(t) = -t^2 + 2 \), and ‘*’ marks the available samples around the peak \( t = 0 \). By only using the maximum value, the time of arrival would be -0.2. However, by interpolating the samples as a second degree curve, and calculate an estimate of the value \( \hat{t} \) where \( y'(\hat{t}) = 0 \), the time of arrival will become approximately 0 (using MATLAB’s function \text{polyfit}). ................................. 24

3.4 The received downlink signal is first demodulated to retrieve the frequency offset \( f_{\text{offset}} \), the BCC and the FN. Finding the frequency offset is seen as a part of the demodulation process. ........................................ 26
3.5 Modulation of the training sequences. Input is bits and output is the complex baseband representation. BCC is used when modulating the 26 bit sequence (uplink).

3.6 Block diagram showing the algorithm to find the TOA for the received signal. The process is iterated over the number of available correlation peaks (M) in the signal. FN is used for the downlink signal, to pin a specific number to the TOA value.

3.7 Block diagram showing the calculations of \( \Delta \), given the true time delay \( \delta \) and the TOA values as input. The result is averaged over the available number of peaks (M).

4.1 The hypothetical locations in the simulation model. Both \( \Delta \) and \( \delta \) are equal to zero due to the symmetry between the four nodes.

4.2 Correlation between the two signals used in the model, followed by peak detection gives the error of the TOA estimate.

4.3 Plot of the (normalized) correlation function for the 64 bit training sequence, without noise. The function is symmetric around zero.

4.4 (a) Plot of the (normalized) correlation function for the 26 bit training sequence (BCC = 1). Both without the impact of noise and with added noise (SNR = -5 dB). (b) Zoom in on the correlation function. The peak is located somewhat to the right of the zero value, due to the influence of the noise.

4.5 Plot showing the RMS due to the impact of noise.

4.6 The RMS for the estimation of \( \Delta \), when averaging over 1, 10 and 100 of each TOA value.

5.1 Components of the receiver. The tuner is a Rohde&Schwarz EB200 Miniport Receiver, and the A/D-DDC system is manufactured by Pentek, Inc. (Model 7152) and programmed by FOI staff.

5.2 A detailed view of how the components in the receivers are connected, in the case for the laboratory trials. For the field experiment, the setup was the same, except for the receivers having their own antenna. The tuners, as well as the 160 MHz signal generator, uses a 10 MHz clock reference as a stabilizer. The 1 PPS (pulse per second) is used to trigger the recording. Since RX1 uses a GPS as reference while RX2 uses a floating reference, the recordings are triggered at different times within the same second, creating a synchronization error between 0 and 1 s.

5.3 Positions for the laboratory trials. A and B marks the spots for the mobile stations. The antenna connected to the two receivers is located on the roof of the laboratory. The area is located south of Linköping University, Linköping, Sweden.

5.4 Positions for the field experiment. The position for the mobile station (MS) is approximately the same as the one used for the laboratory trials (B).
5.5 Absolute value of the received uplink signals from Attempt i. The upper signal is from receiver 1, and the lower from receiver 2. It is possible to see how the amplitude variates in time. Due to this, only the part from approximately 3 - 4.5 s were used to calculate the TOA values. Compare with Figure 5.10.

5.6 Absolute value of the received uplink signals from Attempt iv. The upper signal is from receiver 1, and the lower from receiver 2.

5.7 Histogram over the Δ_{\text{ERROR}} values for Attempt i. The values of Δ_{\text{ERROR}} are multiplied by c to get the results in meters. The mean value is -0.77 m after averaging. The correct value is zero (no error).

5.8 Histogram over the Δ_{\text{ERROR}} values for Attempt ii. The mean value is 0.78 m.

5.9 Histogram over the Δ_{\text{ERROR}} values for Attempt iii. The mean value is -0.94 m.

5.10 The TOA differences for Attempt i. The uplink signal is the signal from the mobile, and the downlink signal is the signal from the base station. As can be seen in the figure, the synchronization error drift in time. Due to this fact, the synchronization error was interpolated as a first order polynomial, instead of the normal averaging.

5.11 The TOA differences for Attempt ii.

5.12 The Δ values from Attempt v. The values seem to oscillate outside the variation in accuracy. The part used for the calculations is about 3 s long.

5.13 Histogram over the Δ values from Attempt iv. The mean value is -70 m. The correct value is -59 m. The sum of the bars is the number of training sequences (M, uplink) used for averaging, in this case 650. Compare with Table 5.4.

5.14 Histogram over the Δ values from Attempt v. The mean value is -140 m.

5.15 Histogram over the Δ values from Attempt vi. The mean value is -169 m.

5.16 Histogram over the Δ values from Attempt vii. The mean value is -100 m.

5.17 Histogram over the Δ values from Attempt viii. The mean value is -256 m.

5.18 Histogram over the Δ values from Attempt ix. The mean value is -120 m.
List of Tables

<table>
<thead>
<tr>
<th>Table</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.1</td>
<td>Frequency bands for GSM 900 and GSM 1800.</td>
<td>9</td>
</tr>
<tr>
<td>2.2</td>
<td>List of different possible training sequences depending on BCC [3GPP, 2013].</td>
<td>11</td>
</tr>
<tr>
<td>5.1</td>
<td>Parameters for the laboratory attempts. ( F_u ) is the uplink frequency.</td>
<td>41</td>
</tr>
<tr>
<td>5.2</td>
<td>Parameters for the attempts in the field experiments.</td>
<td>41</td>
</tr>
<tr>
<td>5.3</td>
<td>Results from the laboratory trials. ( M ) is the number of peaks used for TOA calculations during the call (the number used for averaging).</td>
<td>43</td>
</tr>
<tr>
<td>5.4</td>
<td>Results from the field experiments. The number of training sequences ( M ) used in one attempt depends on the appearance of the signal; only the parts with high amplitude (relative the noise) were used.</td>
<td>47</td>
</tr>
</tbody>
</table>


Arne Norre Ekstrøm and Jan Hvolgaard Mikkelsen. GSMsim: a MATLAB Implementation of a GSM Simulation Platform. Technical report, Aalborg Universitetsforlag, Aalborg University, 1997. Note: To get access to the MATLAB code, contact with the authors is suggested. The URL is not working. Cited on page 23.


