The Detection and Tracking of Portable GSM Handsets Using a 5-Element Circular Array

Jonathan Lambert-Porter

A dissertation submitted to the Department of Electrical Engineering,
University of Cape Town, in fulfilment of the requirements
for the degree of Master of Science in Engineering.

Cape Town, December 2004

Declaration

I declare that this project report is my own, unaided work. It is being submitted for the degree of Master of Science in Engineering in the University of Cape Town. It has not been submitted before for any degree or examination in any other university.

Signature of Author ..... Signed by candidate

Cape Town
22 October 2002

Abstract

Direction Finding (DF) is a process that involves estimating the directions of the arrival for propagating wavefronts impinging on an antenna array from arbitrary directions relative to that antenna array. By understanding how the signals captured relate to the geometry of the DF antenna, one can separate out these signals spatially, and provide their directions of arrival with some degree of certainty.

GSM, the Global System for Mobile Communications is a mobile digital communications system which has rapidly gained acceptance on a global scale since the early 1990s. Because the communications standard is made use of throughout the world today, it would be desirable to investigate the feasibility of the detection and tracking of such signals as an extension for DF platforms that are used by monitoring authorities such as the police or service providers.

This thesis presents and discusses the implications of detecting and tracking GSM mobile handsets. Because the thesis was commissioned by a company that already manufactures broadband surveillance equipment with a particular DF implementation, the thesis approaches the problem with *their* specific implementation in mind assessing its competency in detecting and tracking GSM mobile phones.

To understand the nature of GSM, a simulator was developed to convey information about the structure of the datasets that would be recorded in the field, and is compared to datasets captured with the DF equipment. Conclusions are drawn from the recordings, and recommendations for future work in this field are discussed.

Acknowledgements

I should like to thank the following people for their contributions toward this thesis:

1. Dr. Andrew Wilkinson, my thesis supervisor for the many hours he spent advising and helping me during the duration of this research.
2. My industrial sponsor for supporting this research.
3. The NRF for their support via the THRIP programme.

Contents

List of Figures

List of Tables

List of Acronyms

ARFCN	Absolute Radio Frequency Channel Number
AUC	Authentication Centre
BCCH	Broadcast Control Channel
BSC	Base Station Controller
BSS	Base Station Subsystem
BTS	Base Transceiver Station
CA	Cell Allocation
DB	Dummy Burst
dB	Decibel
DCCH	Dedicated Control Channel
DF	Direction Finding
DOA	Direction of Arrival
EIR	Equipment Identity Register
ESPRIT	Estimation of Signal Parameter via Rotational Invariance Technique
FACCH	Fast Associated Control Channel
FDMA	Frequency Division Multiple Access
FFT	Fast Fourier Transform.
FN	TDMA Frame Number
GMSC	Gateway MSC
GMSK	Gaussian Minimum Shift Keying
GSM	Global System for Mobile Communication

HLR	Home Location Register
HSN	Hopping Sequence Number
IFFT	Inverse Fourier Transform.
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Subscriber Identity
ISDN	Integrated Services Digital Network
LA	Location Area
MA	Mobile Allocation
MAIO	Mobile Allocation Index Offset
MUSIC	Multiple Signal Classification
MS	Mobile Station
MSC	Mobile Switching Centre
MSK	Minimum Shift Keying
NMT	Nordic Mobile Telephone
PCH	Paging Channel
PLMN	Public Land Mobile Network
RF	Radio Frequency
SACCH	Slow Associated Control Channel
SCH	Synchronisation Channel
SNR	Signal to Noise Ratio
TCH	Traffic Channel
TDMA	Time Division Multiple Access
TN	Time Slot Number
UHF	Ultra High Frequency
VHF	Very High Frequency

Chapter 1

Introduction

1.1 Background to Research

Bandwidth in radio communication systems is an expensive commodity for which organisations pay large sums of money. Any individual can potentially transmit in a band, thereby interfering with signals that are legally permitted to occupy the same band. There must be a mechanism in place that will allow authorities to monitor these illegal occupants. If a possible illegal occupier is identified, it would be preferable to be able to infer a direction associated with his / her position by monitoring the RF spectrum, thereby assisting the authorities to apprehend the individual. A Direction Finding (DF) platform allows its user to monitor the RF band, inferring a direction of arrival for content in that band. Several applications for this type of platform exist. Police might require such technology to assist with the recovery of stolen communications equipment. It could also be of use to the military for the detection of possible threats.

GSM, *the Global System for Mobile Communication* is undoubtedly the fastest growing mobile communications system and currently spans over 200 countries. With an unprecedented growth of more than 160 million new customers in the last 12 months, 2 billion users are predicted by the end of 2006 [16]. As the GSM 900 band falls into their band of interest, an industrial company[1] which manufactures DF equipment, commissioned this research to investigate the feasibility of the detection, and direction finding of GSM signals emitted from mobile GSM handsets with their specific DF implementation in mind. A 5-element circular array was to be used to capture the signals, and this DF antenna was connected to a block sampling DF platform for signal acquisition.

[1]The company name cannot be revealed for reasons of confidentiality.

1.2 Problem Definition

Consider the following scenario. A number of cell phones are present in some area; the locations and the numbers in this area are unknown. For the users of the DF equipment, it would be preferable to have some mechanism for detecting the presence of a phone and displaying the direction of arrival (DOA) for the signals emitted from that phone *over time.*

In order to do this, a DF antenna must be used to capture the signals that are emitted from the phones. The captured signals must then be processed accordingly in such a way as to reflect the DOAs for the phones as accurately as possible. An illustration of this is provided in Figure 1.1, which shows two mobile phones moving along separate paths, being monitored by a 5-element DF antenna.

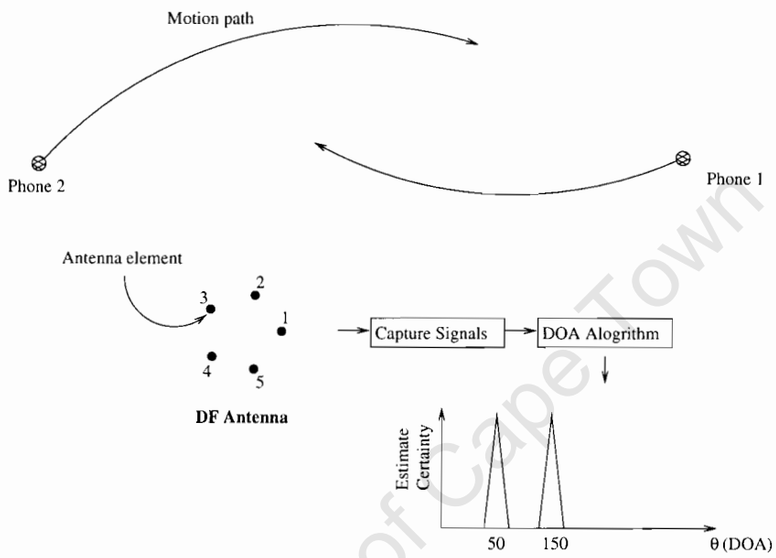


Figure 1.1: Problem Definition Illustration

Once the instantaneous DOA for the each of the phones has been determined, it would be preferable to have some mechanism for classifying which DOAs belonged to which phone, and monitoring the angular position of each phone over time.

Spatial position can be determined by employing two such DF systems, using a triangulation technique to pinpoint the position of an emitter.

1.3 Objectives of the Thesis

The thesis describes an investigation into the detection and the subsequent tracking of mobile GSM transmitters. The aforementioned company have already developed a DF platform with a specific implementation of a correlative DOA algorithm which is applied

to signals captured in the RF band. This thesis investigates the problem of direction finding of GSM handsets *in this context*. Specific objectives include:

- A study of the aspects of the GSM standard that are pertinent to the problem at hand.
- A description of a block sampled, DF platform, assessing the performance and suitability of the DOA algorithm when applied specifically to GSM signals.
- The development of a GSM network software simulator to facilitate the study of recorded datasets.
- A study of the signal propagation delay between the handsets and the base station, and the repercussion this delay has on the recording of GSM signals with the block sampling DF platform.
- The capture and analysis of real datasets.

The thesis is concluded with recommendations for further work to be performed in the tracking of GSM mobile phones.

1.4 Plan of Development

The GSM standard and the direction finding and tracking of RF signals are two separate entities, and are treated as such in the thesis. In order to fully appreciate the nature of the problem at hand, a discussion of the *relevant* aspects of the GSM standard is covered in Chapter 2. Such aspects include the GSM architecture, the network access scheme implementation, handset power control as well as a brief discussion on the security measures implemented in the standard.

Chapter 3 discusses the correlative direction finding technique that was implemented as part of the research, discussing the advantages and disadvantages of the technique.

Because various modules of the hardware were being developed in parallel with the research, a software simulator was developed to determine the effectiveness of the proposed direction finding technique in a GSM environment. The construction of the simulator is discussed in Chapter 4, and the results for various scenarios are presented and discussed.

Anomalies can arise in the GSM signals recorded, as a result of the position of the DF antenna relative to the mobiles in an area and the nature of the DOA algorithm. Chapter 5 presents a short case study of such scenarios, and provides statistics relating the current sampling technique to these worst case scenarios.

Real GSM datasets were captured with the hardware platform in a controlled environment in which several cell phones were positioned around the DF antenna and made to follow certain paths. These results are compared with those from the simulator, and are discussed in Chapter 6 accordingly.

Finally, conclusions are drawn and recommendations for further research are presented in Chapter 7.

Chapter 2

GSM Architecture and Protocols

Introduction

In early 80s, several analogue communications standards existed in Europe. Examples were the *Total Access Communication System (TACS)* in the UK, *NMT* in Scandinavia, and the *C-Netz* in Germany [10]. As these standards were incompatible, service was limited to specific regions hence constraining the development of a European economy of scale. It was realized by the *Central European Posts and Telecommunications Offices,* CEPT that due to the increasing number of subscribers all over Europe, they would be presented with a problem by the early 90s unless a remedy was found.

As a result, the *Group Special Mobile* (GSM) was established to investigate and begin work on the definition of a digital Europe-wide standard. The first GSM networks were launched in 1991 [10].

GSM is a very complex and in-depth standard. This chapter *introduces* the reader to aspects of the standard that are important to understanding the problem at hand i.e. ascertaining the direction of GSM signals. The information presented in this chapter is a summary of the literature reviewed, which was derived and compiled from the following sources [6, 9, 10, 20]. Explanations and definitions have been written as briefly as possible and many aspects of the standard that are deemed irrelevant (such as detailed signalling protocols for call initiation, the processes of subscriber authentication, location updating and encryption), have been omitted. The full definition of the GSM standard may be found at the ETSI web site [4].

The chapter begins by briefly discussing the GSM system architecture as a whole, moving onto the chosen modulation technique. From here the radio access scheme is presented, followed by the network cell planning for a *Public Land Mobile Network* (PLMN). After the allocation of frequencies has been discussed, the implementation of the frequency hopping algorithm across the cellular frequency sets is presented.

To conclude the chapter, the time synchronisation of the mobile station with the base station is considered, and finally the power control of the mobile handset during a conversation is discussed.

Because several acronyms are used in this chapter, it can become difficult to keep track of the different acronyms and their meanings. The reader is asked to refer to the "List of Acronyms" page should confusion arise.

2.1 GSM System Architecture

A GSM system comprises three main subsystems. These are the Network subsystem, Radio subsystem, and finally the Operation and Maintenance subsystem [10]. The components of these subsystems network are illustrated in Figure 2.1.

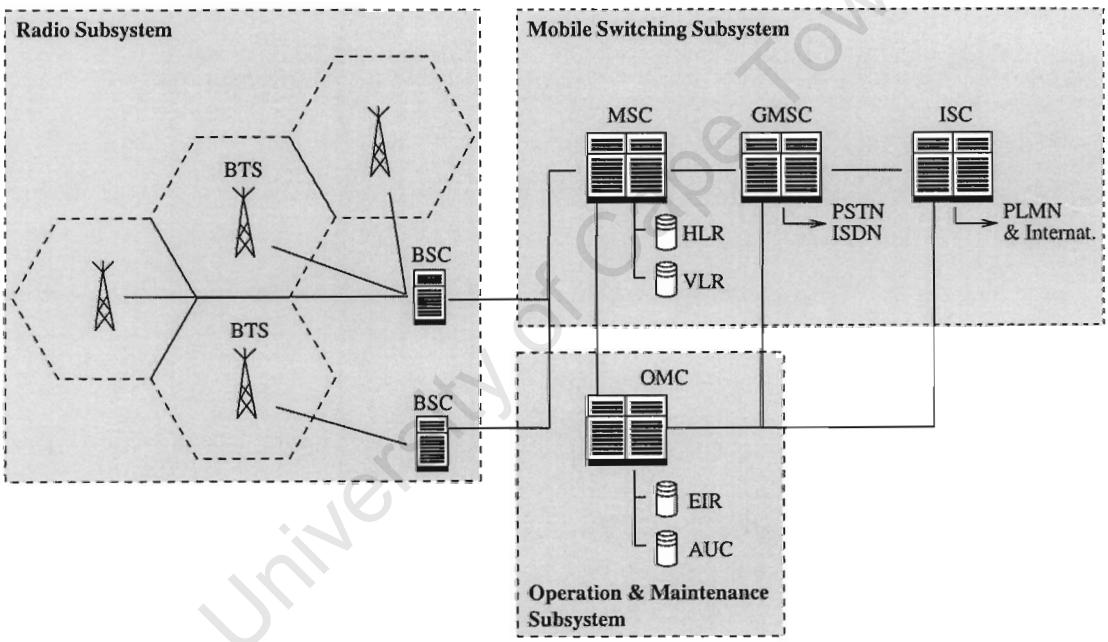


Figure 2.1: Components of a GSM network

2.1.1 Network Subsystem

This includes all the functions associated with end-to-end calls, subscriber management, and the interfacing with other PLMNs and the fixed PSTN. The switching subsystem consists of the *Mobile Switching Centre* (MSC), *Home Location Register* (HLR), *Visitor Location Register* (VLR). The functions of each of these is as follows:

MSC: The MSC is responsible for call setup, routing and handover. The *Gateway MSC* is responsible for routing calls from the fixed networks (ISDN, PSTN) to the mo-

bile networks. Connections to other mobile networks or international networks are routed over the *International Switching Centre* (ISC).

HLR: The HLR is a centralised database that contains *all* subscriber information of the PLMN. It contains fixed entries such as access and service permissions, as well as a link to the corresponding VLR address.

VLR: The VLR is a similar database to that of the HLR but is updated dynamically. A VLR is generally associated with a single MSC, and stores data of all mobiles that are currently in the administrative area of that MSC. As a mobile moves into a new area serviced by a different MSC, an entry in the VLR for the new area is created and after the information from the old VLR has been copied across, the old entry is deleted.

2.1.2 Radio Subsystem

The Radio subsystem is comprised of the *Base Transceiver Station* (BTS), *Base Station Controller* (BSC), and finally the *Mobile Subscriber* (MS). Their functions are as follows:

BTS: The BTS houses a number of transceivers that communicate bi-directionally with the Mobile Subscriber. It is responsible for power control, error correction, as well as limited hand-over decisions for the mobile subscriber.

BSC: The BSC is responsible for coordinating a number of BTSs in an area and contains more sophisticated protocols for hand-over decisions.

MS: The mobile handset contains a SIM card which is unique to the subscriber. The SIM is responsible for storing network-specific data, as well as functions for user authentication and the data encryption keys. The power of the SIM card is that it separates user mobility from equipment mobility, allowing international roaming independent of mobile equipment.

The BTS and BSC form the *Base Station Subsystem* (BSS) which is viewed by the supporting MSC as being an entity responsible for maintaining communication with the mobiles in their coverage area. The BSS as a whole is responsible for radio channel management (channel quality assessment), transmission functions, and hand-over preparation.

2.1.3 Operation and Maintenance Subsystem

The Operation and Maintenance Centre (OMC) is responsible for the network administration (subscriber statistics, load calculations, billing information, maintenance tasks etc).

In addition to this, the *Equipment Identity Register* (EIR) and the *Authentication Centre* (AUC) exist within the subsystem, and are responsible for:

AUC: Confidential subscriber keys are stored in this database, which are used to generate further keys for authentication and cryptographic processing. These are passed to and from the VLR during on a per call basis.

EIR: This database stores the serial numbers of the mobile stations (IMEI number).This makes it possible for network operators to monitor the stations, or in certain cases, to bar service access for handsets that have been reported as stolen.

This concludes the section of the GSM Architecture. The Gaussian Minimum Shift Keying Modulation (GMSK) will now be presented and discussed.

2.2 Gaussian Minimum Shift Keying Modulation (GMSK)

The selection of a modulation scheme in any communications system is very important as several design trade-offs exist. Aspects to consider include bandwidth consumption, and the complexity of the modulation and demodulation hardware.

GMSK is an angle modulation technique and was adopted because firstly, the power spectrum is compact with low adjacent channel interference, and secondly, the signals have constant amplitude simplifying the amplifier design (there are no special linearity requirements in the amplifier). It is similar to MSK, but makes use of a low pass Gaussian frequency filter before the phase modulation which leads to a more compact power spectrum.

The raw enciphered bit stream undergoes several processing steps before it is modulated. These are shown below in Figure 2.2 and will be dealt with separately.

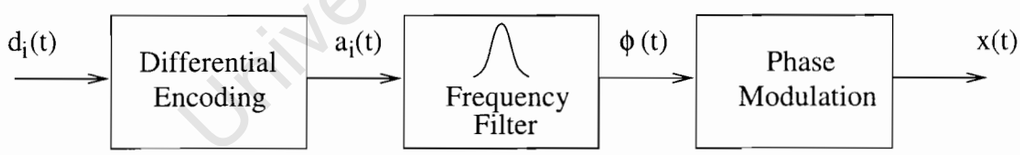


Figure 2.2: GSM Digital Modulation

2.2.1 Differential Encoding

The bit stream to be modulated is differentially encoded as follows [6]:

$$\hat{d}_i \quad = \quad (d_i + d_{i-1}) mod 2, \qquad d_i \in (0,1) \tag{2.1}$$

From here, the bipolar input stream $a_i(t)$ is formed. This is essentially a sequence of Dirac pulses.

$$a_i \quad = \quad 1 - 2\hat{d}_i \tag{2.2}$$

The bipolar stream is fed into the frequency filter that as defined as follows.

2.2.2 Frequency Filter

The frequency filter, $g(t)$ is essentially the convolution of a Gaussian low-pass filter, $h(t)$ with that of a rectangular step function. The definitions of these are as follows:

$$g(t) \quad = \quad h(t) \otimes rect(t/T) \qquad \text{where:} \tag{2.3}$$

$$rect(t/T) = \begin{cases} 1/T & |t| < T/2 \\ 0 & |t| \geq T/2 \end{cases}, \qquad T = 1/(270.8 * 10^3)\, s \tag{2.4}$$

$$h(t) = \frac{1}{\sqrt{2\pi}\sigma T} exp\left(\frac{-t^2}{2\sigma^2 T^2}\right), \qquad \sigma = \frac{\sqrt{ln2}}{2\pi BT}, \qquad BT = 0.3 \tag{2.5}$$

Note that the constants B and T are the 3 dB bandwidth of the filter $h(t)$ and the bit duration of the incoming bit stream. The resulting frequency filter $g(t)$ is illustrated in Figure 2.3.

At this point, the reader may be wondering why a value of $BT = 0.3$ was chosen for the Standard. As BT is decreased, the lobe of the impulse response $g(t)$ becomes broader. While this leads to a more compact power spectrum, the time domain inter-symbol interference becomes greater as the individual bits from the bit stream become "smeared" in the time domain.

2.2.3 Phase Modulation

The weighted impulse train mentioned in Section 2.2.1, is convolved with the impulse response $g(t)$. The instantaneous frequency, $\omega_i(t)$ is found as follows:

$$\omega_i(t) \quad = \quad \sum_i a_i \pi \eta g(t - iT) \tag{2.6}$$

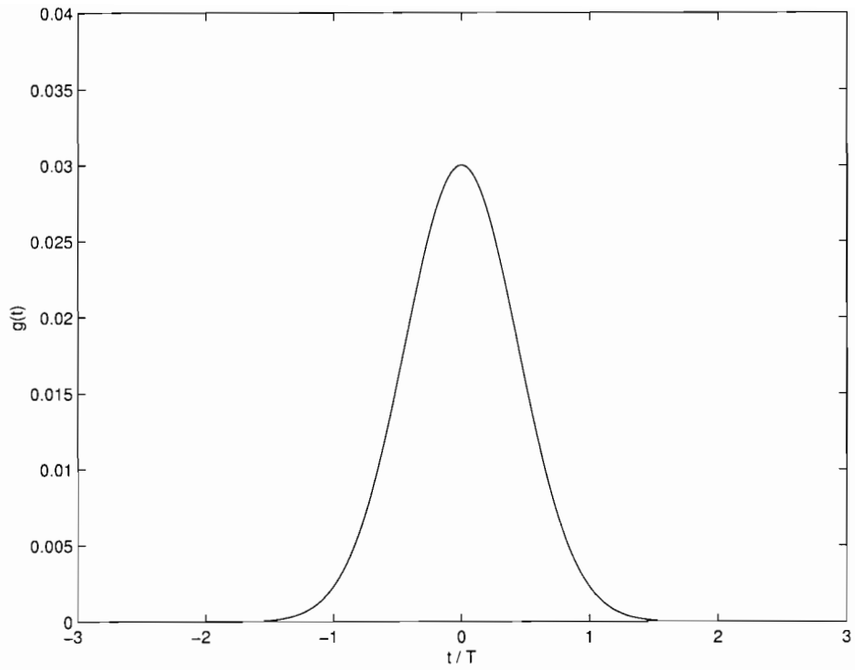


Figure 2.3: Impulse response $g(t)$ of the frequency filter

The phase of the modulation signal is then derived from the instantaneous frequency as follows [6]:

$$\phi(t) = \int_{\tau=-\infty}^{t} \omega_i(\tau) d\tau \tag{2.7}$$

The modulation index, η is chosen to be 1/2 such that the maximal phase shift per bit is $\pi/2$. Once the phase has been obtained, it is fed to a phase modulator, where the carrier signal $x(t)$ is expressed as follows:

$$x(t) = Acos(2\pi f_o t + \phi(t) + \phi_o) \tag{2.8}$$

The phase for a basebanded[1], 148 bit waveform GMSK waveform is illustrated in Figure 2.4. The FFT of a 148 bit GMSK waveform (at a bit rate of 33.9 kbit/s) is shown in Figure 2.5.

[1]The basebanded analytic representation is $x(t) = Ae^{j(\phi(t)+\phi_o)}$

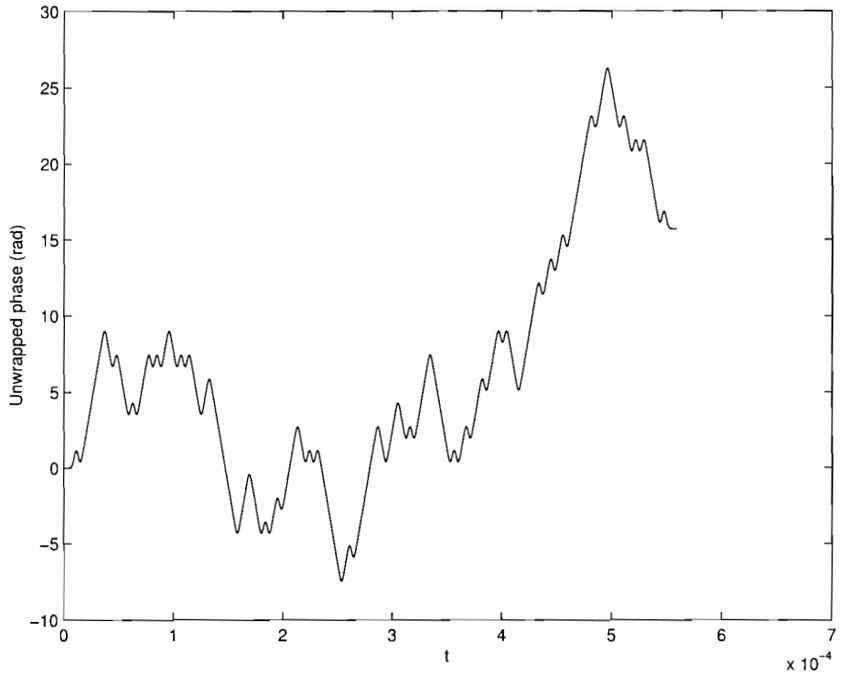


Figure 2.4: Phase Function of a 148 bit GMSK signal

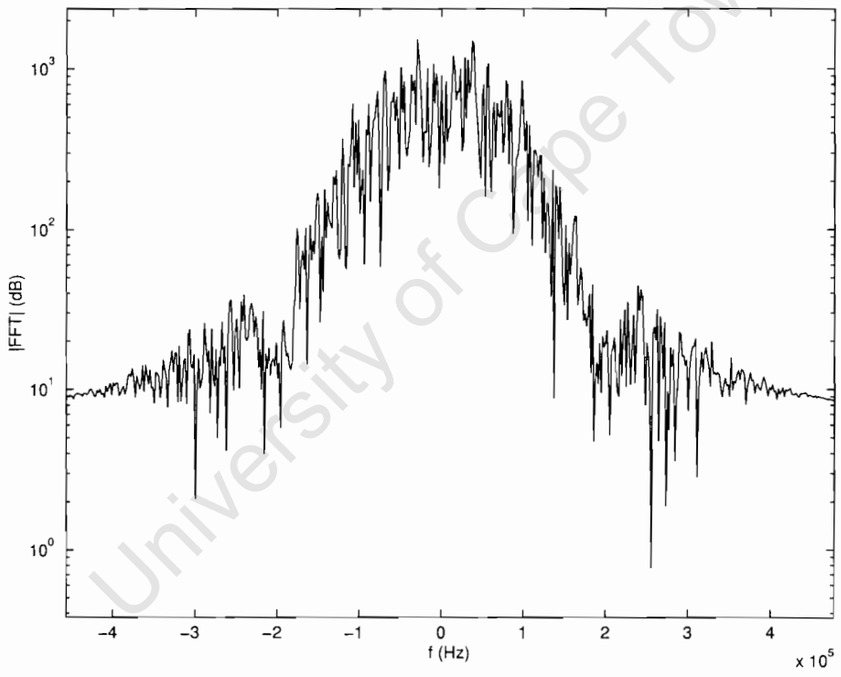


Figure 2.5: |FFT| of a GMSK Waveform

Notice how the phase smoothly varies over time. This results in the compact spectrum illustrated in Figure 2.5. The significance of 148 bits will be discussed later in this chapter.

2.3 TDMA / FDMA Access Scheme

GSM employs a combination of Time Division Multiple Access (TDMA) and Frequency Division Multiple Access (FDMA) schemes. The access scheme makes use of two frequency bands, namely the uplink (mobile to base station) and downlink (base station to mobile) bands. These occur from 890 to 915 MHz and 935 to 960 MHz respectively. The bands are divided up into 125 narrow band carrier channels, each 200 kHz wide. These channels are called *Radio Frequency Channels* (RFCHs), and are defined at frequency values:

$$\text{Uplink:} \qquad F_u(n) = 890.2 + 0.2(n-1) \text{ MHz} \qquad (1 \leq n \leq 124)$$

$$\text{Downlink:} \qquad F_d(n) = 935.2 + 0.2(n-1) \text{ MHz} \qquad (1 \leq n \leq 124)$$

Note that n is known as the *Absolute Radio Frequency Channel Number* (ARFCN). A pair of channels with the same ARFCN form a duplex communication channel separated by 45 MHz. The reason the first frequency channel from each band is unused (890 on the uplink and 935 MHz on the downlink), is because they serve as a protection mechanism against neighbouring out-of-band interference. The access scheme is illustrated in Figure 2.6.

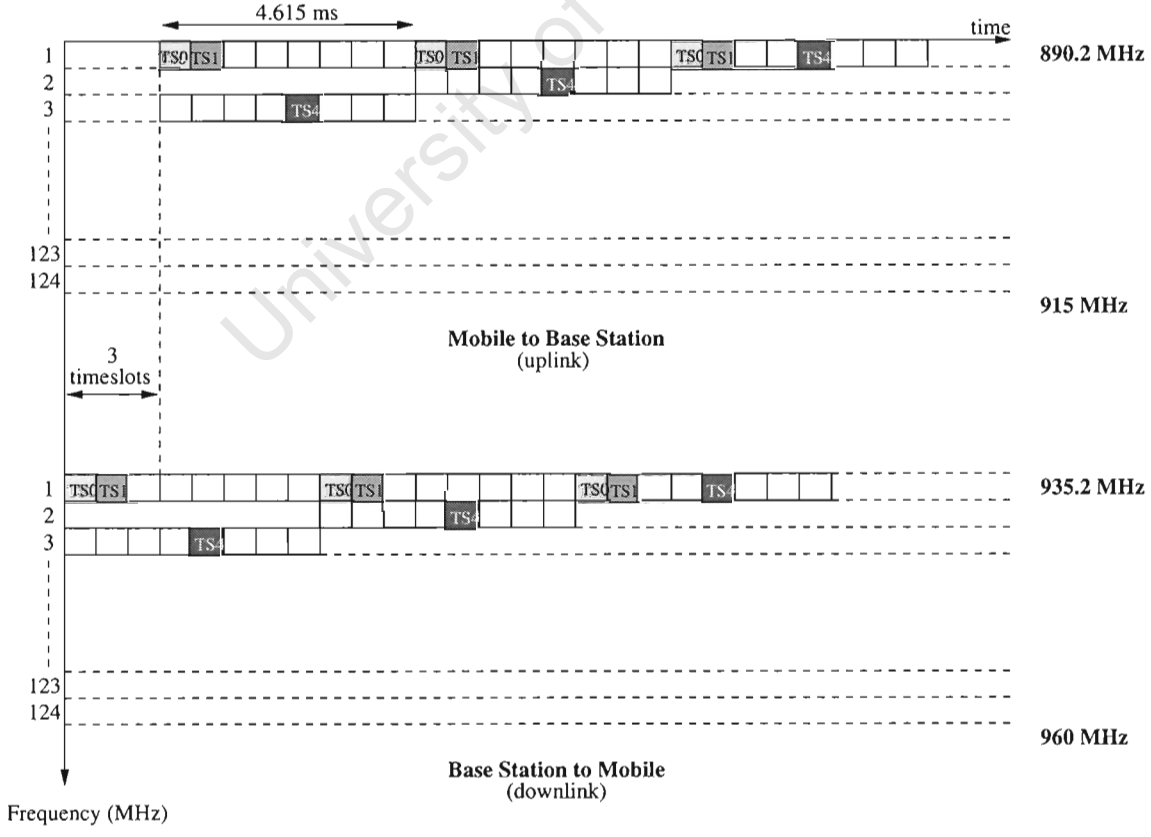


Figure 2.6: TDMA, FDMA Access Scheme

A subset of these radio frequency channels, the *Cell Allocation (CA),* is allocated to the

base station. One of the frequencies in the Cell Allocation is used for broadcasting information from the base station to the mobile stations. The remainder of the frequencies in the CA are allocated to the mobile stations, and are known as the *Mobile Allocation (MA).* Cell Allocation planning will be covered later in the chapter.

One TMDA frame comprises 8 time slots. Each time slot lasts approximately $577\mu s$, corresponding to a burst of length of 156.25 bits (148 data bits, followed by 8.25 guard bits) per slot. This translates to a gross bit rate of 33.9 kbits/s per time slot. A phone is dynamically allocated a time slot at the start of a conversation, and maintains this time slot for the duration of the call (unless a hand-over occurs which is described later). We may think of this as the allocation of a *physical channel* (one time slot per TDMA frame on a particular frequency channel). A *logical channel* is then mapped on top of the physical channel. In the case of speech, fax, or data transmission, the logical channel is referred to as a *Traffic Channel* (TCH).

The mobile station transmits information back to the base station *approximately* 3 time slots after a downlink transmission[2]. This allows for the phone to have a single transceiver unit, as data reception and transmission occur at separate times. The timing diagram in Figure 2.6 is not entirely accurate as the propagation delay between the base station and the mobile has been ignored. The propagation delay between the base station and the mobile stations in an area can pose a problem to the direction finding algorithm and is addressed in more detail later in Chapter 5.

Figure 2.6 illustrates three traffic channels allocated to TS0, TS1 and TS4. Slow frequency hopping changes the transmission frequency at the end of each TDMA frame in an attempt to average the interference over the MA. This feature may be turned on and off by the base station after the allocation of a new traffic channel. The phones that have been allocated TS0 and TS1 are not frequency hopping, but the phone in TS4 is. It should also be noted that the mobile station may be allocated a new traffic channel if the phone is handed over to a new base station, or if the bit error ratio of the current traffic channel reaches unacceptable levels due to slow fading. The details of slow frequency hopping and hand-over are discussed in more detail later.

2.4 Logical Channel Mapping

As mentioned earlier, a logical channel is a virtual channel that is mapped onto a physical channel. There are numerous types of logical channels which are multiplexed into two main frame structures to take advantage of the TDMA scheme. The first is a 26-frame multiframe comprising 26 TDMA frames, and the second is a 51-frame multiframe

[2]Data packets are released by the mobile unit such that they arrive at the base station at the correct times without collision.

comprising 51 consecutive TDMA frames. The 26-frame multiframe is used for speech and data transmission, and the 51-frame multiframe is used predominantly for signalling between the mobile station and the base station. The frame hierarchical structure is illustrated in Figure 2.7.

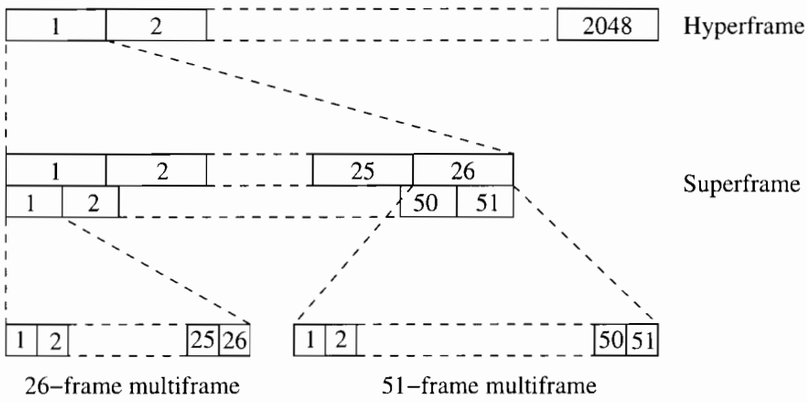


Figure 2.7: GSM Multiframe Structure

A superframe consists of $50 \times 26 = 1326$ TDMA frames, and a hyperframe consists of 2048 superframes.

Each TDMA frame is given a unique *frame number* (FN) between 0 and 2 715 615. This is cyclic and is incremented at the end of each frame. The FN repeats every 3 hrs, 28 min and 52s and is used as an input for the ciphering and deciphering of bit streams, and for the slow frequency hopping algorithm.

Because the 51-frame multiframe is used essentially for signalling between the base station and the mobile while the phone is in idle mode (listening to the current base stations and assessing the quality of service from surrounding base stations), its structure will not be considered in this thesis.

2.4.1 The 26-Frame Multiframe

The 26-frame multiframe comprises 26 TDMA frames and is used predominantly for speech and data transfer. Two types of logical channels are multiplexed in this frame structure onto the same physical channel. These are the traffic channel (TCH), and the *Slow Associated Control Channel* (SACCH). The structure of a 26-frame multiframe is illustrated in Figure 2.8.

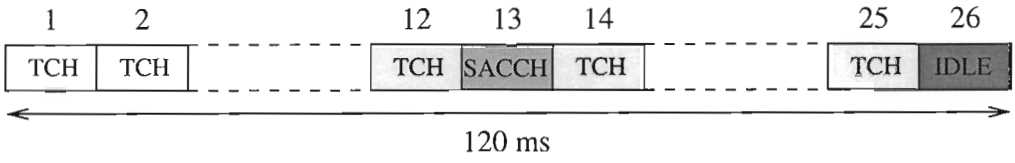


Figure 2.8: 26-frame Multiframe Structure

The purpose of the TCH and SACCH is as follows:

Traffic Channel:

A traffic channel, as already mentioned, is used for the transfer of speech and data. If the channel is fully utilised, it is known as a full rate traffic channel (TCH/F). Speech is transmitted at 13 kbit/s, with data transmitted at 12 kbits/s, 6 kbits/s and 3 kbits/s. To accommodate more subscribers, the channel may also be split into two half-rate channels (TCH/H). The bit rates for the TCH/H are half that of the TCH/F.

Slow Associated Control Channel:

The SACCH is one of a number of control channels that is used for signalling information between the BTS and the MS. It is a bi-directional channel and has a number of functions associated with it. Measurement reports of the received signal strength from the serving BTS as well as adjacent BTSs are relayed back to the serving BTS. This information is required for hand-over decisions. It is also carries information regarding the power regulation for the MS as well as the timing synchronisation information for both the uplink and downlink. If there is no signalling data to transmit, the MS transmits the results of the radio signal level measurements. Details of the timing synchronisation, and channel quality assessment are covered later in the chapter.

Fast Associated Control Channel:

The FACCH is assigned with a TCH and works in "stealing mode." If urgent signalling transmission must take place during a call, approximately 20 ms worth of TCH bursts are "stolen" from the 26-frame multiframe and replaced with signalling information. This occurs during a hand-over from one cell to another.

The IDLE frame in Figure 2.8 is reserved for SACCH use if 2 TCH/H subscribers are present rather than one TCH/F subscriber. It also allows the mobile to listen to and decode surrounding base station information because the ratio of the different multiframe formats (26 frame vs 51 frame) has the effect that the relative position of the IDLE frame shifts

by exactly one frame every 240 ms (2 × 26TDMA frames) with regard to the 51-frame multiframe.

2.4.2 Burst Structure for Traffic and Signalling Channels

GSM defines five different burst types that are used for data transmission and signalling information (normal burst), as well as for access and synchronisation with the network (frequency correction, synchronisation, access and dummy bursts). We are interested primarily in the normal burst as this is the burst used to transmit information on the traffic and control channels mentioned earlier.

The structure is of a normal burst is illustrate in Figure 2.9.

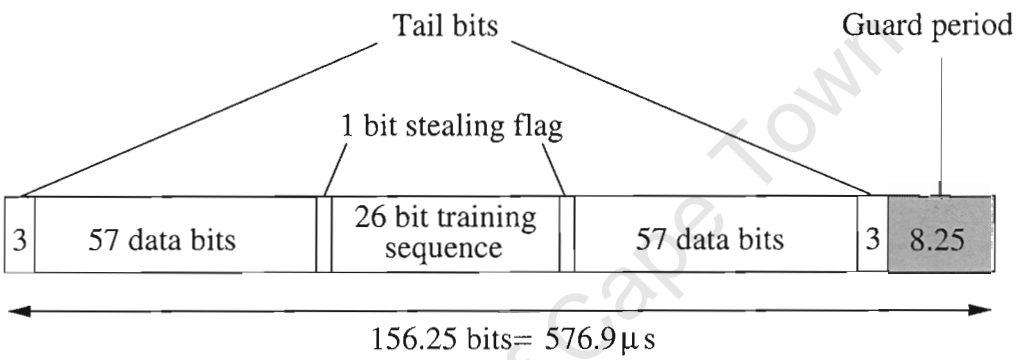


Figure 2.9: Normal burst

Each burst starts and finishes with 3 tail bits set to a logical "0." The stealing bits are used to indicate whether the burst contains traffic data or signalling data. The training sequence in the middle of the burst is used for channel estimation to optimise reception with an equaliser and for synchronisation [6]. Finally the guard period at the end of each burst ensures that transmissions in 2 consecutive timeslots do not interfere with each other at the base station.

2.5 Network Planning

Recall from Section 2.3, that the GSM900 bandwidth for the uplink and downlink bands is 25 MHz each. Considering the uplink band, potentially with 124 narrow band channels, and 8 time slots per band, $124 \times 8 = 992$ physical channels are available for subscriber allocation. How then is it possible to provide service for several thousand subscribers? The solution is to spatially separate and reuse the frequencies.

Spatially separating and reusing the frequencies involves dividing a geographical area into smaller areas (cells) and assigning each cell a set of frequencies (CA as mentioned

earlier). This set is then reused in another other cell where the co-channel interference between the cells is sufficiently small. From a design viewpoint, the cells are assumed to be hexagonal. In practice though, because the edge of the cell is a line of equal power between adjacent BTSs, cells are irregular in shape and size.

2.5.1 Frequency Reuse Distance

How far apart the cells should be spaced such that the frequencies can be reused? Consider Figure 2.10.

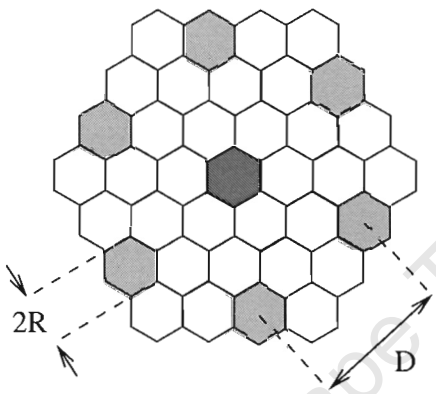


Figure 2.10: Cellular Network Model

If we assume a hexagonal model, the worst case *Carrier to Interference Ratio* (CIR) occurs when 6 surrounding BTSs (using the same frequency sets) are all interfering with the BTS in the middle of the cluster (darkest hexagon in Figure 2.10). Assuming that they all transmit equal powers, the CIR at the cluster centre can be shown to be [9]:

$$W \approx \frac{1}{6}\left(\frac{R}{D}\right)^{-\gamma} \qquad D > R \tag{2.9}$$

where:

R: Radius of a cell

D: Distance between cells with the same frequency set

γ**:** Propagation coefficient (typically of the order of 4)

For a desired CIR at a given cell radius, one has to choose a minimum distance D for the frequency reuse above which the co-channel interference falls below the required threshold [6].

2.5.2 Cluster Formation

Clusters are formed by distributing the subsets of available frequencies over a *number* of cells, rather than one (as was indicated in Figure 2.10). The size of a cluster is characterised by the number of cells per cluster k, which determines the frequency reuse distance D. Examples of cluster sizes are shown in Figure 2.11.

(a) k = 7 (b) k = 3

Figure 2.11: Cluster Formation for Frequency Reuse

A cluster can potentially contain ALL the frequencies of the available bandwidth. Typically however where there are several PLMNs in a country, the GSM bandwidth is split accordingly. Frequency sets may only be reused in neighbouring clusters (i.e. no frequency may be reused within a cluster).

By considering the cluster constant k, the frequency reuse distance D can be shown to be [6]:

$$D = R\sqrt{3k} \tag{2.10}$$

Substitution of Equation 2.10 into Equation 2.9 yields :

$$W = \frac{1}{6}(3k)^{\frac{\gamma}{2}} \tag{2.11}$$

What this means is that for a given CIR (typically 18 dB for good speech understandability [6]), and an approximate propagation coefficient $\gamma = 4$, the minimum cluster size:

$$\begin{aligned} 10logW &\geq 18\,dB \\ W &\geq 63.1 \end{aligned}$$

$$D \approx 4.4R \tag{2.12}$$

Substituting Equation 2.12 into Equation 2.10 results in $k \geq 6.5$, implying that $k = 7$.

This means that for $W = 18\,dB$, a reuse distance $D = 4.6R$ is needed [9]. One should note that as the cluster size k increases, the frequency reuse distance D increases and a larger CIR is achieved. However, because the set of frequencies in a cluster is finite, an increase in k also reduces the number of physical channels per cell, and thus the number of subscribers per cell.

The reuse distance issue has been addressed, but the selection of the CA has not been discussed. This essentially involves probabilistic traffic calculations (the number of subscribers in a given area) which won't be presented in this thesis. Typically however, a BTS is allocated three to five radio carriers, carrying between 24 and 40 simultaneous communications [10].

2.6 Slow Frequency Hopping

Mobile radio suffers frequency-selective fading due to multipath propagation phenomena. This means that the transmitted signal from a mobile may be severely attenuated at the base station depending on the frequency dependent propagation path between the mobile and the base station. In order to average these effects, GSM provides an *optional* frequency hopping procedure known as "slow frequency hopping." Slow frequency hopping changes the carrier frequency after each burst approximately 217 times per second (this corresponds to the 1/TDMA frame duration). In contrast, fast frequency hopping changes the carrier frequency at the start of each bit in the burst.

If the BSC notices that a particular channel is failing for a mobile station, it can instruct a mobile to start hopping by instructing the BTS to pass it the whole RF channel set (MA) rather than just one RF channel from the set. The phone then uses this set with the hopping algorithm that is built into the phone, and starts hopping across the frequency sets without further instruction from the BTS.

Different hopping patterns exist. One is cyclic hopping, where the mobile simply cycles through the frequencies in the set; and the other is a pseudo-random pattern. Theoretically, if N frequencies were available to the mobile, $N!$ different non-repeating sequences could be constructed. GSM however, offers 64 sequences [10] to be constructed and a particular pattern is selected by specifying the *Hopping Sequence Number,* (HSN). The *Mobile Allocation Index Offset,* (MAIO) is an index to the MA and specifies which frequency in the MA group with which to start the hopping algorithm.

All mobiles in a cell bear the same HSN and make use of the same frequency set. Each

mobile however, will be allocated different MAIO values at the start of frequency hopping. For example, if the MA consisted of ARFNs: $MA = [2, 5, 12, 18]$ and two phones were in the same cell on time slot 1, they would have to be allocated different ARFCNs to avoid interference. Let us assume phone one was allocated ARFCN 5 and phone two, ARFCN 2 from the MA set. The corresponding MAIO values would be 1 for phone one, and 0 for phone two (since $0 \leq MAIO \leq length(MA) - 1$). The nature of the hopping algorithm makes it impossible for two mobiles on the same time slot, bearing the same HSN but different MAIO values to hop to the same frequency.

Adjacent cells in the same cluster make use of the same HSN since these cells use different frequency sets. In areas where frequency sets are reused, different HSNs are used to improve interference diversity. The actual hopping algorithm will now be discussed.

2.6.1 Slow Frequency Hopping Algorithm Implementation

Before presenting the actual hopping algorithm, the following parameters are defined [10]:

N: The number of frequencies in MA: $1 \leq N \leq 64$

MAIO: This determines the next frequency where the mobile will hop to: $0 \leq MAIO \leq N - 1$

HSN: If $HSN = 0$, then hopping will be cyclic across the MA, else it will be pseudo-random: $0 \leq HSN \leq 63$

FN: The TDMA frame number mentioned in Section 2.4 is received from the base station during synchronisation of the mobile with the network, and is decomposed into three variables $T1$, $T2$, and $T3$. These are calculated within the mobile as follows (div denotes integer division):

T1: $FN\, div\, (26 \times 52)$: $0 \leq T1 \leq 2047$

T2: $FN\, mod(26)$: $0 \leq T2 \leq 25$

T3: $FN\, mod(51)$: $0 \leq T3 \leq 50$

NBIN: The number of bits required to represent Integer($log_2(N) + 1$)

RNTABLE: A look-up table of 114 integer values whose values lie between 0 and 127.

The flow chart for the hopping algorithm may be found in the Appendix and is taken directly from Mehrotra [2]. A new MAIO is computed after each iteration of the hopping algorithm. The phone then tunes to the new ARFCN, which is obtained from MA[MAIO].

Slow Frequency Hopping Illustration

The pseudo-random nature of the hopping algorithm is illustrated in Figure 2.12 with time on the vertical axis, and the MAIO on the horizontal axis. One phone is hopping across 4 frequencies in the MA. Please note that Figure 2.12 does not illustrate actual GMSK signals, but rather serves to illustrate a hopping sequence. The sequence in Figure 2.12 was derived using a randomly selected HSN of 15, and a FN which was set to 4000. The horizontal lines in the image illustrate the start of a new TMDA frame.

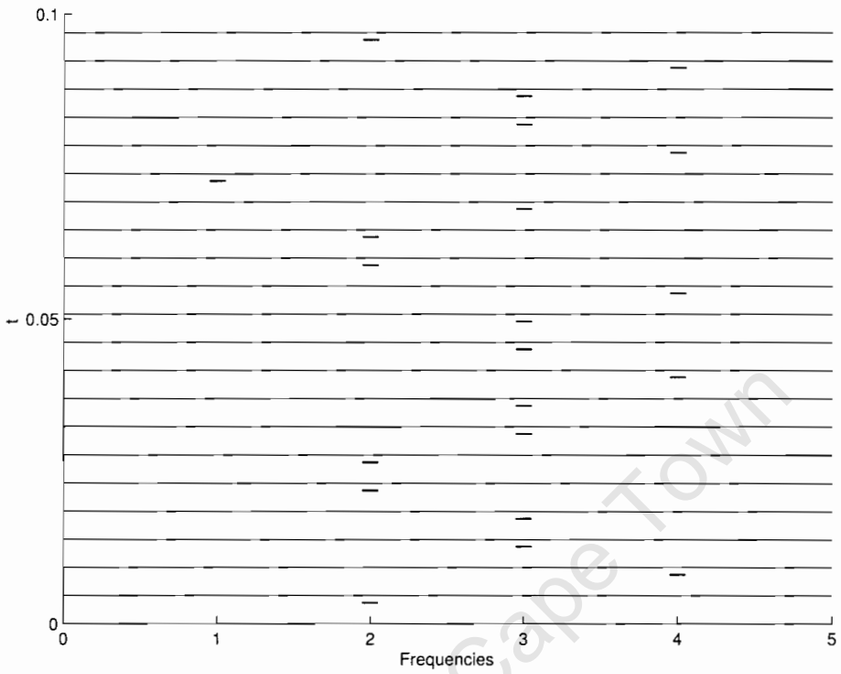


Figure 2.12: Pseudo-random Slow Frequency Hopping

It is interesting to note that the phones do not always hop to a new frequency after each burst, and appear to maintain the same carrier for up to three TDMA frames.

2.7 Mobile Station Timing Synchronisation

One of the flexibilities that the GSM standard offers is mobility. This means that a mobile station can be anywhere within a cell, and move around within that cell. As a result, the distance between the mobile and base station may vary during a call. Recall from Section 2.3, that when the base station transmits a burst to a mobile on the downlink band, it expects a burst from that particular mobile exactly three time slots later on the uplink band. Because of the distance fluctuation, if the phone transmits back to the base station 3 time slots after it has received information, the bursts received at the base station would not be aligned correctly and would interfere with each other. An example of this is

illustrated below in Figure 2.13.

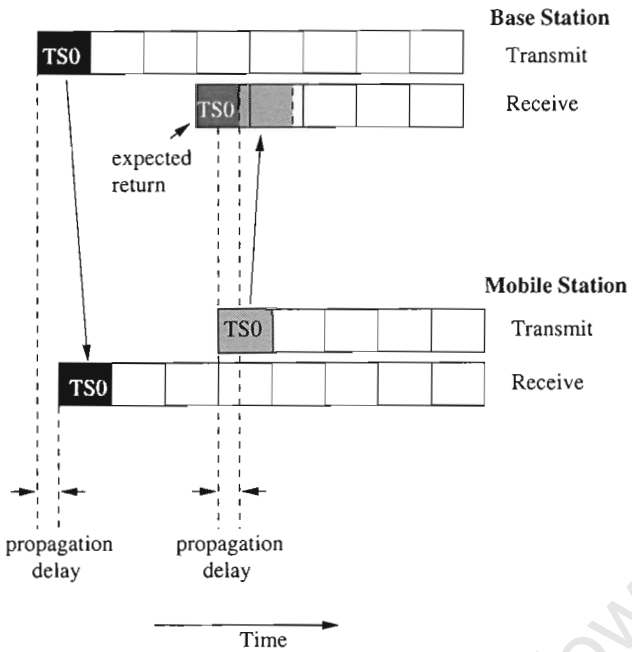


Figure 2.13: Two way propagation time slot interference

As can be seen from the diagram, a burst is transmitted from the base station to the mobile on TS0. A short time later, the mobile receives the burst and transmits a burst back to the base station 3 time slots later. Instead of the base station receiving a return 3 time slots later after it transmitted, the return from the mobile station interferes with the return of TS1.

To avoid time slot collisions, the internal timing mechanism of the phone is adjusted in proportion to the distance the handset is from the base station. In order to this, the base station monitors the propagation delay between the phone and the base station, and sends a message to the phone to advance its internal mechanism to compensate for the ***two way*** propagation delay.

There are 64 steps for timing advance which are coded 0 to 63. Step 0 implies no timing advance i.e. the transmission to the base station occurs exactly 3 time slots, or 468.75 bit durations later with regard to the downlink. Such a situation exists when the phone is close to the base station. At step 63, the timing mechanism is advanced by 63 bit durations, such that the transmissions back to the base station are transmitted with a delay of 405.75 bit durations relative to the start of the downlink.

With this in mind, the maximum **one way** propagation time corresponds to 31.5 bit periods ($\approx 113.3\,\mu s$). This corresponds to a maximum distance between mobile and base station of 35 km. Therefore a GSM cell may have a maximum diameter of 70 km. The timing advance is illustrated in Figure 2.14.

In order to ensure that the mobile remains synchronised with the BTS, the amount of

serving BTS. This occurs when full bidirectional point to point transmission takes place for example during a call, when the phone is authenticating (registering with the network) or when the phone is updating its location. From a direction finding perspective, it would be difficult to fix a position on a phone that is authenticating with the network due to the short time that the authentication procedure requires (relative to say the duration of a phone call). As a result, we will not concern ourselves with the details of authentication or location updating, and will only consider what events take place during a conversation where the mobile would be transmitting for several seconds.

2.8.1 Channel Measurement

As mentioned earlier, bi-directional signalling information takes place over the SACCH during a conversation. One single SACCH block lasts 480 ms, and comprises 4 TDMA frames in 4 consecutive 26-frame multiframes (c.f. Figure 2.8). Two parameters are determined to classify the channel during a connection, the *Received Signal Level,* RXLEV and the *Received Signal Quality,* RXQUAL.

The received signal power is continuously measured by both the MS and the BTS and lies in the range -110 dBm to -48 dBm. These levels are averaged over time, and are transmitted in a portion of the SACCH block together with the timing synchronisation between the BTS and the phone (c.f. Section 2.7). RXQUAL is measured as a bit error ratio in percent before error correction occurs, and again is determined by averaging. The transmission of these values back to the BTS allows BTS to assess the downlink quality of the channel.

During a mobile station's unused timeslots, the 6 neighbouring broadcast carriers are scanned and decoded and the measured signal levels are passed back to the BTS for handover decisions.

2.8.2 Power Control

In order to preserve the life of the mobile station's battery, it would be desirable for the mobile station to transmit on the lowest power necessary to maintain an acceptable BER at the base station. As a result, the mobile station's transmitter power is controlled in steps of 2 dBm by the base station. Sixteen power control steps are defined for this purpose: Step 0 (43 dBm = 20 W) to Step 15 (13 dBm). Depending on the power class of the mobile, the transmitter power of the mobile is increased from Step 15 up to its maximum value by the base station. The GSM power classes are given in Table 2.1 and indicate the maximum peak transmission power [6].

The transmitter power of the base station can also be controlled in steps of 2 dBm (apart

Power Class	Mobile Station W (dBm)	Base Station W
1	20 (43 dBm)	320
2	8 (39 dBm)	160
3	5 (37 dBm)	80
4	2 (33 dBm)	40
5	0.8 (29 dBm)	20
6	-	10
7	-	5
8	-	2.5

Table 2.1: GSM power classes

from the broadcast carrier which remains constant to allow for comparisons by the mobile stations), so as not to saturate the receiver amplifiers of the mobile station.

Recall that RXLEV and RXQUAL are used to assess the quality of the radio link. The network defines upper and lower bound thresholds, and determines from these thresholds and the averaged RXLEV and RXQUAL whether to increment or decrement the power level accordingly.

Because it has been shown that during a call a speaker speaks less than 40% of the time, battery life can further be conserved by turning off the transmitter. A voice activity detector is used to detect the presence of speech, and when no speech is detected the transmitter is turned off. This is known as *Discontinuous Transmission* (DTX).

2.9 Hand-over

Hand-over is defined as being the transfer of an existing channel to a new channel of either the same BTS (*Intra-cell Hand-over)* or a different BTS (*Inter-cell Hand-over).* There are four main reasons why hand-over occurs [10]:

1. Maintenance of high signal quality.
2. Recovering co-channel interference.
3. Traffic balancing among cells.
4. Recovering in the event of failure of a control channel.

Without going into the details of hand-over decisions, there are three cases of hand-over:

1. Hand-over from one radio channel to another of the same BSC (same or different BTS).

2. Hand-over between channels of the same MSC but different BSC.

3. Hand-over between different MSCs.

There are several thresholds that are drawn upon when deciding whether a hand-over should occur or not. The major criterion in decreasing order of priority are the integrated and averaged RXQUAL and RXLEV values on both the uplink and downlink, distance, and finally a power budget calculation that estimates the path loss between the mobile and the serving and surrounding BTSs.

There are two modes of hand-over, synchronous and asynchronous. In synchronous hand-over, the old and new cells are synchronised so that their TDMA timeslots start at exactly the same time. This allows the MS to internally compute the timing advance for the new cell as it is simply twice the difference in arrival times between the old and the new BTS.

In asynchronous mode however, the old and new cells are unsynchronised, and the BTS is required to compute the timing advance for the MS which it then transmits back to the MS. For this reason, asynchronous hand-over takes 200 ms as opposed 100 ms for synchronous hand-over.

2.10 Data Encryption

At this stage, the reader may be wondering why we can't make use of the signal information that is emitted from the mobile in an attempt to gain information from the transmission that may help determine where the mobile resides. Without going into the details of GSM security, GSM provides four security services:

1. **TMSI assignment:** A temporary number assigned to a mobile each time a subscriber requests a location updating procedure, call attempt or service request that is used to identify and page the subscriber.

2. **Authentication:** A Challenge and Response technique used to identify confirm subscriber identify

3. **Encryption:** Signalling data between the BTS and mobile is encrypted using a 64 bit cipher key and the 22 bit frame number (mentioned earlier) to produce two, 114 bit encryption code words S1 and S2 that are used to encrypted payload data.

4. **SIM card and Mobile Equipment Identity number (IMEI)**: Ensures no stolen equipment or unauthorised equipment is used to access the network.

To undo the encryption would present a very difficult problem, and as the research was aimed at trying to detect and infer a direction on the signal emissions from the mobile, the actual information at a bit level would not be relevant.

Chapter 3

The Block Sampling, Correlative Direction Finding System

3.1 Introduction

"Direction Finding" is a term that is used to describe the process of estimating the angular direction of arrival (DOA) of an emitting source using an antenna array comprising two or more elements. Since the 1960s, substantial research in this area has been conducted and several methods have been proposed for ascertaining the directions of arrival (DOA) for several types of signals [3, 19, 5].

The first of direction finding techniques involved manually sweeping the DF antenna and noting the direction for which the received signal strength was a maximum. Today, with the advent of high powered personal computers, Eigen value decomposition algorithms such as *Multiple Signal Classification* (MUSIC) and *Estimation of Signal Parameter via Rotational Invariance Technique* (ESPRIT) can be applied to direction finding problems to obtain highly accurate DOA estimates of signals immersed in Gaussian white noise [5, 8].

Since the objective of the thesis is to evaluate the effectiveness of the correlative DOA estimation technique being implemented by the company's DF hardware, this chapter will present and discuss the adopted correlative technique, illustrating its strengths and weaknesses.

The chapter begins by introducing the principles of direction finding, moving on to present the DF platform and a derivation of the adopted correlative DOA algorithm. From here, a discussion on the actual implementation of this algorithm is presented which includes a discussion related to the characterisation of the DF antenna, and an investigation into the structure of both simulated and real characterisation tables. Once characterisation has been covered, the application of the algorithm is presented and the output of the

algorithm is discussed. A brief study of its performance related to the antenna geometry in varying signal to noise ratio environments is then presented. After this, a discussion on the application of the algorithm to the GMSK signals used in the GSM 900 Standard is covered, highlighting situations where the algorithm may break down. To conclude the chapter, a discussion of how a-priori GSM related frequency information may be combined with the correlative DF algorithm is presented.

3.2 The Principles of Direction Finding

Before discussing the actual DF technique, it would be useful to explain briefly the principles of direction finding with particular reference to the Generalised Cross Correlation (GCC) method of direction finding [7]. This method of direction finding is similar to that implemented on the DF platform, and will be presented as a model from which to derive the correlative DF algorithm. Aspects to consider include a brief derivation of how a direction of arrival is estimated for an incoming plane wave, antenna element spacings, and the number of antenna elements required to infer an unambiguous direction of arrival.

3.2.1 Inferring a Direction of Arrival Using Two Elements

Most DOA techniques make use of the instantaneous phase differences between the elements of the DF array. Because of the spacing of the antenna elements, the wavefront arrives at each element with a time delay that is dependent on its direction of arrival. This time delay, is referred to as the time difference of arrival (TDOA), τ. If τ can be determined, the location of the source would be constrained to the set of points in space corresponding to the given TDOA [11].

Consider the simplest DF antenna, a two element antenna (elements 1 and 2) separated a distance D as shown in Figure 3.1 (note the definitions of the angles). Suppose a source is emitting some signal, $s(t)$ at some DOA θ, and the signals recorded on elements 1 and 2 are $s_1(t)$ and $s_2(t) = s_1(t - \tau)$ respectively.

If we inspect the Fourier transform of $s_2(t)$,we observe that:

$$S_2(\omega) = S_1(\omega)e^{-j\omega\tau} \tag{3.1}$$

$S_2(\omega)$ is essentially identical to $S_1(\omega)$ but with a frequency dependent phase shift applied to the Fourier domain of the signal. If we could undo this phase shift, then $S_2(\omega)$ would be equal to $S_1(\omega)$. By forming the conjugate product of the two signals, we are left with:

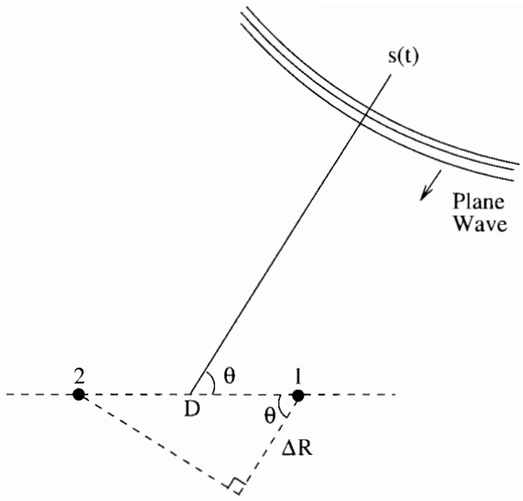


Figure 3.1: Simple Two Element DF Array

$$S_1(\omega)S_2^*(\omega) = S_1(\omega)S_1^*(\omega)e^{j\omega\tau} \tag{3.2}$$

If we now multiply Equation 3.2 by a phase correction factor, $e^{-j\omega\tau_\theta}$, where τ_θ is the TDOA for a particular DOA θ, the $e^{j\omega\tau}$ term in Equation 3.2 would be cancelled when $\tau_\theta = \tau$. If the function is also integrated over ω, the signal energy would be maximised at this particular direction of arrival as $S_1(\omega)S_1^*(\omega) = |S_1(\omega)|^2$. We can therefore define a function, $F(\theta)$:

$$F(\theta) = \int_\omega S_1(\omega)S_2^*(\omega)e^{-j\omega\tau_\theta}d\omega \tag{3.3}$$

$$= \int_\omega S_1(\omega)S_2^*(\omega)e^{-j\omega\tau_\theta}d\omega \tag{3.4}$$

A DOA estimate, $\hat{\theta}$ can be defined as:

$$\hat{\theta} = \arg\max_\theta \{F(\theta)\} \tag{3.5}$$

If we assume the wavefront hits element 1 first at time $t = 0s$, $\omega\tau_\theta$ may be found using trigonometry:

$$\omega\tau_\theta = \frac{2\pi c\tau_\theta}{\lambda}$$

$$
\begin{aligned}
&= \frac{2\pi\Delta R}{\lambda} \\
&= \frac{2\pi D cos\theta}{\lambda}
\end{aligned} \tag{3.6}
$$

where c represents the propagation in free space, and D represents the element spacing.

3.2.2 Antenna Element Spacing

Because $-\pi \leq arg(e^{-j\omega\tau_\theta}) < \pi$, a constraint is placed on D such that $D < \frac{\lambda}{2}$ at the maximal frequency (ω_{max}). This is because $max(\omega\tau_\theta)$ occurs at the DOA where one element is directly behind the other i.e. when $\theta = 0$ and when $\omega = \omega_{max}$. Substituting these values into Equation 3.6, we see that:

$$
\begin{aligned}
\frac{2\pi D}{\lambda} &< \pi \\
D &< \frac{\lambda}{2}
\end{aligned} \tag{3.7}
$$

3.2.3 Inferring a Direction of Arrival Using N Elements

So far, only two antenna elements have been considered. The problem with using only two elements is that it is impossible to distinguish between a wavefront approaching from some angle, θ and another angle $-\theta$ (for example 90° and 270°) because the time delays, and thus the phase differences between the elements would be identical.

A further problem is that of *Shadow Loss*. Consider an incoming wavefront at 0°. Element 1, is directly "behind" element 2 at this angle, and is said to be shadowed by it. This could result in erroneous DOA readings as very little of the signal may be received on element 1.

As a result, the model proposed in Equation 3.6 is extended to incorporate N elements [11]. If we define $t = 0s$ as the time a wavefront hits a particular antenna of the array from a certain DOA, the time difference for the wavefront to hit the rest of the elements can be computed and stored in a vector of time delays, T_θ, for that unique DOA. The time differences between each antenna pair can then be computed by extracting the appropriate time delays from T_θ. The pairwise correlations are summed as follows:

$$
\begin{aligned}
F(\theta) &= f(T_\theta) \\
&= \sum_{k=1}^{N}\sum_{l=1}^{N}\int_\omega S_k(\omega)S_l^*(\omega)e^{-j\omega(\tau_k-\tau_l)}d\omega
\end{aligned} \tag{3.8}
$$

where τ_k and τ_l are the kth and lth elements of the vector of time delays T_θ.

Choosing the number of elements and their arrangement on the DF antenna is application specific. Three elements should be the used as a minimum to avoid DOA phase ambiguities and to compensate for shadow loss at particular DOAs. For example, if three elements were arranged in a triangular fashion, although shadow loss would occur at particular DOAs, the two other element pairs would always be unaffected.

Generally speaking, the more elements one has on the DF antenna, the more robust the DOA measurements are to the effects of noise as better estimates can be obtained from the independent sets. This is however governed by a law of diminishing returns because there comes a point after which addition of further elements will not make a significant difference to the precision of the DOA estimation. One should also realize that the signal processing time increases with an increasing number of elements.

3.3 The Block Sampled DF Hardware Platform

Before mentioning the actual implementation of the DOA algorithm, some time should be spent understanding the hardware platform as a whole which will help clarify the explanation of the DOA algorithm. The DF antenna is presented first, followed by a discussion of the block sampling scheme. To conclude this section, a diagram is presented showing inter-connectivities and signal processing stages before the correlative DOA algorithm is applied.

3.3.1 Circular Five-Element DF Antenna Array

The sampling hardware makes use of five antenna input channels. A simple five element antenna was designed and constructed that would allow for the adequate acquisition of GSM signals. The elements are arranged in a pentagram fashion as depicted in Figure 3.2.

The elements themselves are tuned monopoles (approximately quarter wavelength) and are positioned onto a ground plate. Field patterns for a monopole positioned onto an infinite ground plane have been derived [15]. An infinite ground plane would be impractical for a detection and tracking application, and was reduced to a circular disk with a radius of 15 cm. Reducing the size of the ground plate, affects the directivity of the antenna. A further complication is that the elements are not spaced in the centre of the ground plate.

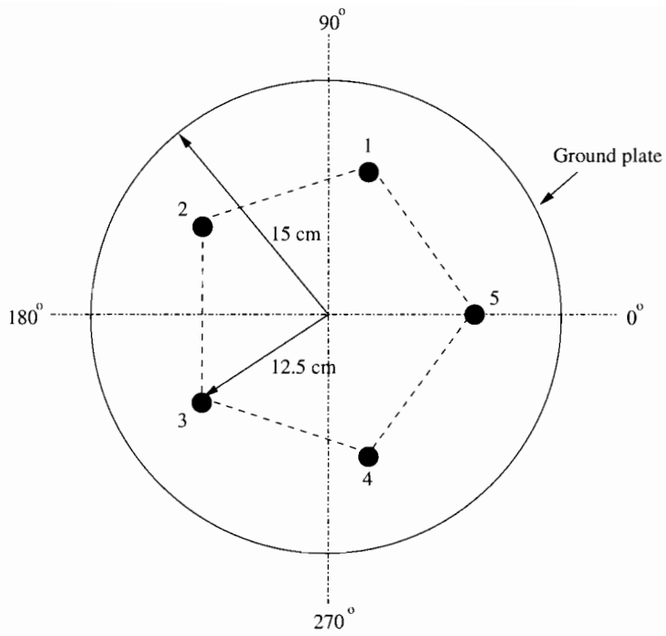


Figure 3.2: The five element DF antenna array

Antenna Polar Pattern

If we observe the polar pattern of a single monopole centred on an infinite ground plane, we would observe a similar pattern to that in Figure 3.3.

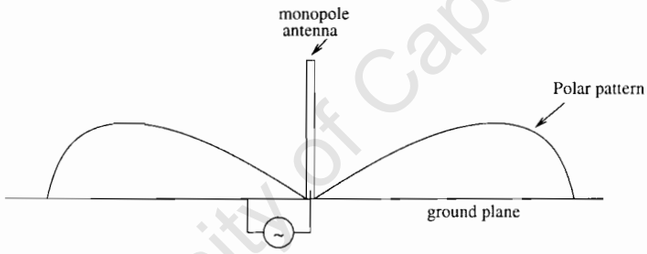


Figure 3.3: Far field pattern for an infinite ground plane

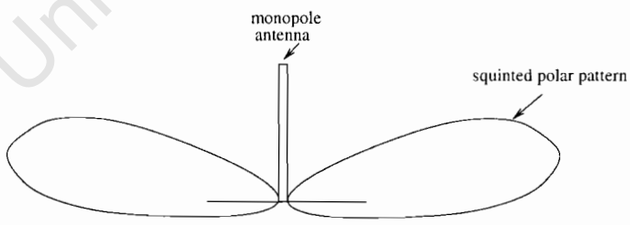


Figure 3.4: Far field pattern for a reduced ground plane

By reducing the size of ground plane, the boresight vector is squinted upwards slightly as depicted in Figure 3.4. In addition to this, signals that would previously have been

undetectable as a result of an infinite ground plane would be now visible as more of the monopole is in view from underneath the antenna.

Power Reflection

The input impedance for a tuned monopole is approximately equal to 37.5 Ω [15]. It would seem reasonable to expect an input impedance close to this value for each of the channels. The input impedance of the coaxial cable between the antenna switch and the antenna (matched to the antenna switch) is 50 Ω.

Let us consider the situation when the antenna is used in transmission mode. The voltage reflection coefficient is defined as the ratio of voltage in the reflected wave to that in the incident wave on the load, as is given by [15]:

$$\begin{aligned} \rho &= \frac{R_L - Z_0}{R_L + Z_0} \\ &= \frac{37.5 - 50}{37.5 + 50} \\ &= -0.143 \end{aligned} \tag{3.9}$$

The power reflection coefficient, ρ^2 indicates how much power is reflected at the load. Squaring Equation 3.9 yields $\rho^2 = 0.020$. This means that approximately 2% of the incident power at the antenna is reflected back to the antenna source.

To verify this, the antenna was constructed and plugged into a network analyser for assessment. The analyser provides a *return loss* plot, which is indicative of the power reflection at the antenna in transmit mode across a range of frequencies. The antenna element lengths were adjusted such that minimum power reflection occurred at approximately 922 MHz for each of the 5 channels. This is the arithmetic mean of the uplink and downlink bands for the GSM 900 spectrum. A plot of the return loss similar to that observed from the network analyser is shown in Figure 3.5.

At at resonant frequency of 922 MHz, $\rho^2 = -18\,dB$ was observed, which translates into a power reflection of 1.6%. This is very close to the predicted value of 2%, making the antenna suitable for practical use.

3.3.2 Block Sampling Scheme

Because continuous sampling generates a huge amount of recorded data, a block sampling scheme was implemented by the company, which allows for the storage of recorded datasets recorded over several minutes. Each of the five channels are sampled in parallel at

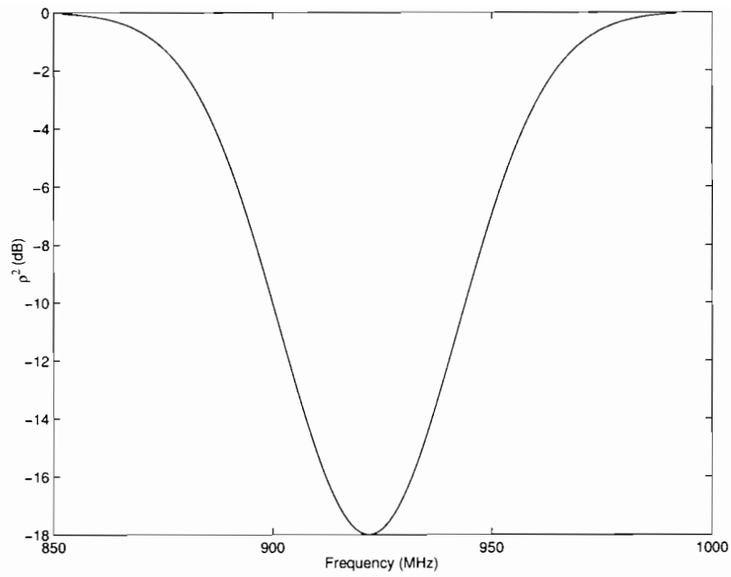


Figure 3.5: Plot of ρ^2 vs Frequency for Single Monopole Antenna Channel

an effective sample rate of 12.8 MHz per antenna channel. Time domain data is sampled in 40 or $80\mu s$ blocks depending on the desired frequency resolution and frequencies over the band 30 MHz - 3 GHz may be investigated. Table 3.1 lists the two most commonly used options:

Sample Capture Time	**Bandwidth**	**Freq. Resolution**	**FFT Size**
$40\mu s$	10 MHz	25 kHz	400
$80\mu s$	10 MHz	12.5 KHz	800

Table 3.1: Hardware Sampling Options

This dataset for each of the captured channels is then FFTd, spectrally filtered and truncated according to which recording option is selected.

Spectral filtering of the dataset is required because the length of the capture window is less than that of a TDMA burst, and as a result, frequency domain ringing can occur due to the premature truncation of the GMSK signal. Consider the FFT of a basebanded GMSK waveform, with a capture window that is wide enough to capture the entire signal transmission. The magnitude of the FFT for the first 2 MHz of the band, is shown in Figure 3.6.

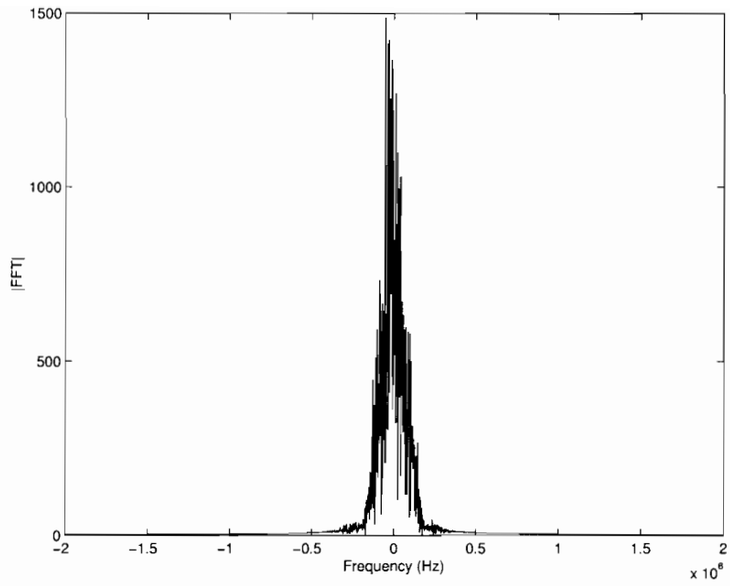


Figure 3.6: |FFT| of a fully captured GMSK Waveform using a $560\ \mu s$ window

Let us now reduce the size of the capture window from approximately $560\mu s$ to $80\mu s$. If we arbitrarily select $80\mu s$ of time domain data from the GMSK waveform, and then perform a FFT on that portion, sidelobes across the frequency band are observed in Figure 3.7.

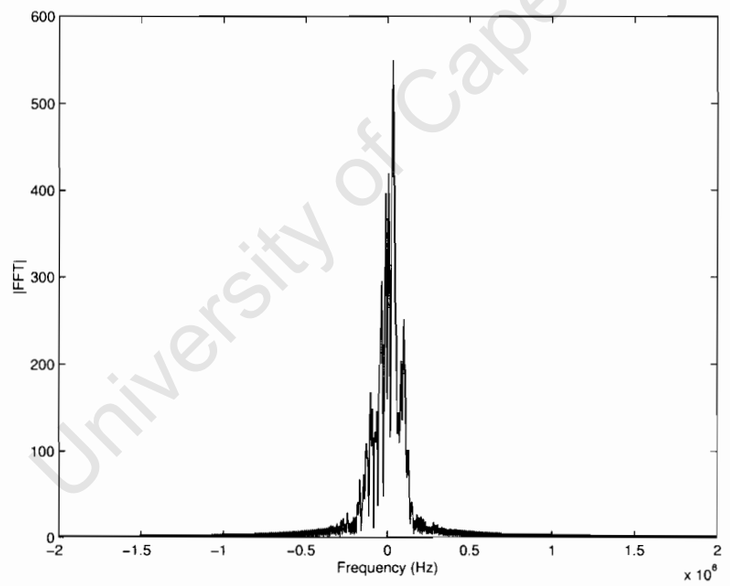


Figure 3.7: |FFT| of a portion of GMSK Waveform captured with $80\ \mu s$ window illustrating sidelobes

To lessen the effects of the ringing, a Blackman Window [1] is applied to the dataset. Comparing Figure 3.7 with Figure 3.8, we can see that the sidelobes have been sup-

pressed.

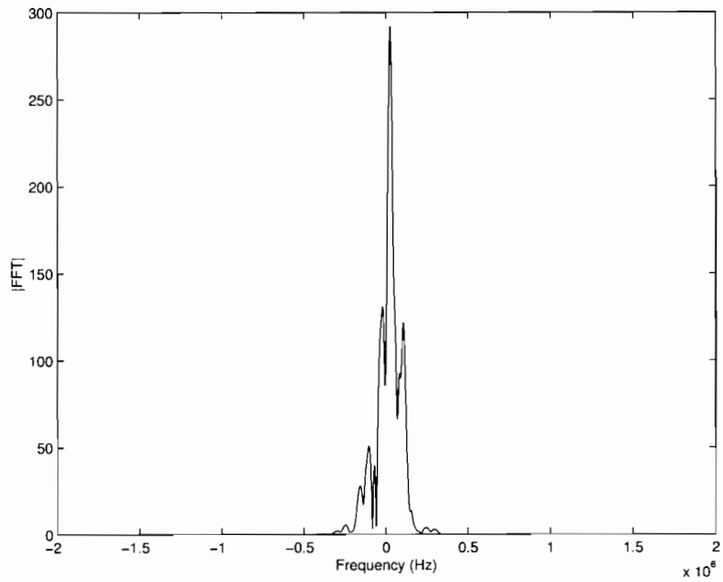


Figure 3.8: |FFT| of truncated dataset after application of Blackman Window

The down conversion, windowing, and FFTing of the data sampled on the five antenna elements results in a 2 ms delay between successive $80\,\mu s$ captures. The $80\,\mu s$ capture window is generally used for recording as the $40\,\mu s$ capture window results in a reduced frequency resolution.

To summarise, a diagram showing the signal processing stages is presented in Figure 3.9.

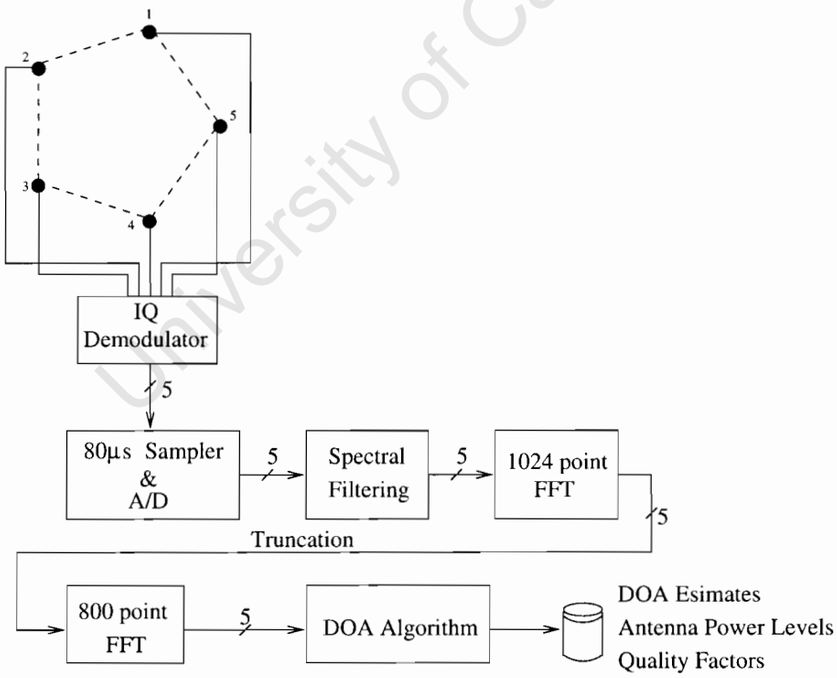


Figure 3.9: Signal Processing Stages for the DF Platform

At the end of each capture performed, the DOA estimates, antenna signal power levels, and the *Quality Factors* (a measure of the certainty of the DOA estimate) are written to disk. The quality factor will be discussed in more detail later.

3.4 The Correlative Direction of Arrival Algorithm

3.4.1 Introduction

The correlative DOA algorithm essentially compares the recorded phase differences between various combinations of antenna elements pairs, with a table of pre-computed phase differences and provides a measure of the correlation and the estimated directions of arrival for which the correlation is strongest. In this way, it is very similar to the GCC method described briefly in Section 3.2.

A common DF technique, known as standard Delay and Sum beamforming (DSB), seeks to combine the signals recorded on the antenna elements in such a way that they add constructively resulting in a maximum power output at the estimated direction of arrival [19, 13]. Depending on the type of antenna array used, a narrow beam can be steered through a full $360°$, allowing the antenna to "look" in a certain direction. Very briefly, the output of the beamformer is given by [5]:

$$x(\theta) = \sum_{n=1}^{5} s_n(t) a(\theta_n) \tag{3.10}$$

where n represents the nth element, $s_n(t)$ represents are the signals recorded on the each of the elements for some incoming wavefront, and $a(\theta_n)$, is the *steering vector*. The steering vector attempts to maximise $s_n(t)a(\theta_n)$ and thus represents a conjugate of the expected signals for the nth element for all θ. The estimated DOA is given by $\hat{\theta} = \arg\max_\theta \{x(\theta)\}$.

Let us assume an incoming wavefront at $0°$. For the circular five element array configuration mentioned earlier, a polar plot of $|x(\theta)|$ is depicted in Figure 3.10.

The main lobe at $0°$ is fairly broad which means that weak signals at $15°$ for example, would be lost in the main lobe (angular resolution is poor). A further problem is that the three sidelobes are approximately equal to half the gain of the main lobe, which means that in low SNR environments, false DOA detections could occur if this lobes exceed that of the major lobe.

For the correlative direction of arrival algorithm to work correctly, signals impinging on the DF antenna are assumed to differ in frequency. The algorithm will later be shown to

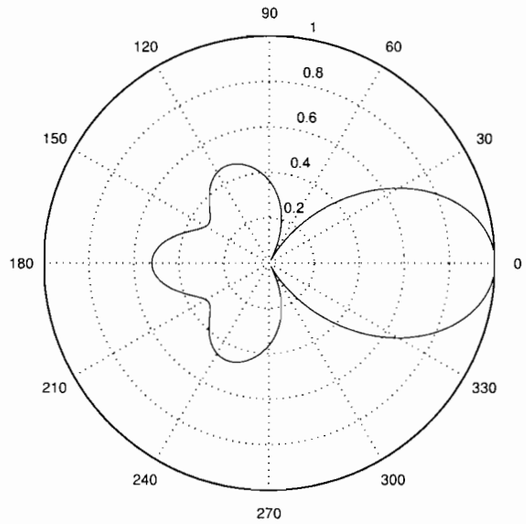


Figure 3.10: $|x(\theta)|$ for DSB using the Circular Five Element DF Array

break down if two or more signals of the same frequency fall on the DF antenna at the same time.

3.4.2 Correlative DOA Algorithm Definition

The correlative algorithm implemented on the DF platform, is similar to that of the GCC method given by Equation 3.8. Recall from Section 3.2.3, that for the GCC method, integration is performed over the entire frequency spectrum for a particular DOA. The implemented correlative algorithm however, does not integrate over the spectrum, but rather isolates each frequency component of the signal spectrum. Again, we define a vector of time delays, T_θ for some DOA θ. Equation 3.8 is reduced to:

$$C(\omega, \theta) = \sum_{k=1}^{N} \sum_{l=1}^{N} S_k(\omega) S_l^*(\omega) e^{-j\omega(\tau_k - \tau_l)} \tag{3.11}$$

where τ_k and τ_l are the kth and lth elements of the vector of time delays T_θ.

If we inspect Equation 3.11 carefully, we can see that all possible combinations of antenna sensors are considered. This is inefficient as no useful information is gained by repeating antenna combinations as the phase information for the product $S_k(\omega)S_l^*(\omega)$ is simply a negative replica of the repeated antenna pair $S_l(\omega)S_k^*(\omega)$. For example, the phase difference for antenna pair (1,4) is exactly the same as antenna pair (4,1), but the phase difference for latter is simply negated.

At this point, we now define an antenna pair as an *aperture*. Because there are five an-

tenna elements, there are 10 unique apertures which may be formed (without element repetition). These are classified as either *pentagram* apertures, or *pentagon* apertures and are so named because of the geometrical pattern the elements in each group form (depicted in Figure 3.11 which show pentagram, and pentagon apertures).

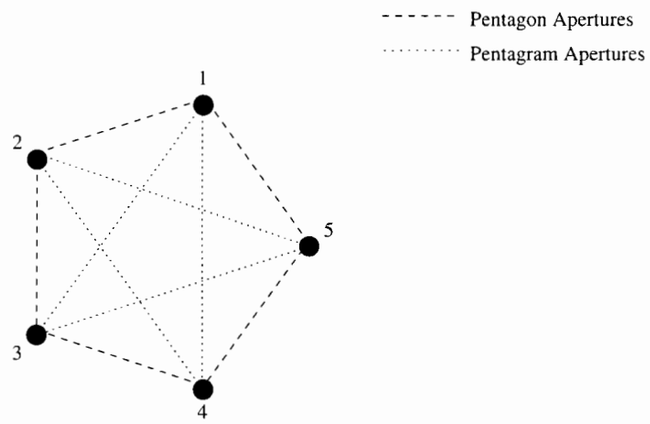


Figure 3.11: Geometrical representation of Pentagram and Pentagon Apertures

Let us define these apertures as follows (antenna element numbers are taken from Figure 3.2):

Aperture	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8	a_9	a_{10}
Antenna Pair	1,4	2,5	3,1	4,2	5,3	1,5	2,1	3,2	4,3	5,4

Table 3.2: Pentagon and Pentagram Aperture List

where apertures a_{1-5} are pentagram apertures, and a_{6-10} are pentagon apertures. We will define $S_n(\omega)$ as:

$$S_n(\omega) = S_k(\omega)S_l^*(\omega) \qquad n = 1 \ldots 10 \tag{3.12}$$

where $S_k(\omega)$ and $S_l(\omega)$ are the Fourier transforms of the signals captured on the elements for the (k, l) antenna pair of the a_nth aperture, and n refers to the aperture number. Let us also define $T_\theta(n)$ as being a vector of time *differences* for the nth aperture at some DOA θ.

Equation 3.11 may now be modified to:

$$C(\omega, \theta) = \sum_{n=1}^{10} S_n(\omega)e^{-j\omega T_\theta(n)} \tag{3.13}$$

The term $e^{-j\omega T_\theta(n)}$ is essentially a phase correction factor for $S_n(\omega)$ computed over various DOAs. When $e^{-j\omega T_\theta(n)}$ is computed at the exact DOA θ for which the signal $s(t)$ is impinging on the antenna, $C(\omega, \theta)$ is a purely real quantity. In practice however this is not the case, as the antenna does not behave in an ideal way. Element spacings are never exact, and as a result the phase information present in $S_n(\omega)$, does not match the theoretical phase information of $e^{-j\omega T_\theta(n)}$ for some modelled antenna geometry. More accurate DOA estimates would be obtained if the phase information were obtained directly from the signals recorded on the *real* antenna for each of the apertures over all DOAs. This process is known as *characterisation* of the antenna and will be investigated in more detail later.

For every nth aperture we can define a characterisation function $V_n(\omega, \theta)$ which is a table of pre-computed gain and phase correction values for every aperture at a given frequency ω and a given DOA θ such that:

$$V_n(\omega, \theta) = |V_n(\omega, \theta)| \, e^{j\phi_n(\omega,\theta)} \tag{3.14}$$

where $|V_n(\omega, \theta)|$ is the magnitude of the characterisation function, and $\phi_n(\omega, \theta)$ is the associated phase. Equation 3.13 may now be updated to reflect the correlation table such that:

$$C(\omega, \theta) = \sum_{n=1}^{10} S_n(\omega) V_n^*(\omega, \theta) \tag{3.15}$$

The normalised complex correlation coefficient is defined as:

$$C(\omega, \theta) = \frac{\sum_{n=1}^{10} S_n(\omega) V_n^*(\omega, \theta)}{\sqrt{\sum_{n=1}^{10} |S_n(\omega)|^2 \cdot \sum_{n=1}^{10} |V_n^*(\omega, \theta)|^2}} \tag{3.16}$$

Recall that for a DOA perfect match, $C(\omega, \theta)$ is purely real as $arg\{S_n(\omega)\} = \phi_n(\omega, \theta)$ and when normalised, $C(\omega, \theta) = 1$. It therefore makes sense to consider only the real part of the correlation product. The estimator is used to produce a direction estimate for *each* frequency component present in the captured signal and is given by:

$$\hat{\theta}(\omega) = \arg\max_{\theta} \{\Re e\{C(\omega, \theta)\}\} \tag{3.17}$$

We define the factor $Q(\omega, \theta) = \Re e \{C(\omega, \theta)\}$ as a measure of match and will be referred to as the *quality factor* of the estimate where: $-1 \leq Q \leq 1$.

This concludes a derivation for the correlative direction of arrival algorithm that is implemented by the company. The following section discusses the practical implementation of Equation 3.16.

3.5 Practical Implementation of DOA Algorithm

3.5.1 Discrete Algorithm Definition

For the algorithm proposed in Equation 3.16 to be implemented on digital signal processors, it must be made discrete. The signals captured on the antenna elements are automatically made discrete in the frequency domain by the FFT operation. Similarly, the characterisation function must also be made discrete. It would be impossible and practically infeasible to process *every* DOA. As a result, DOAs in intervals of δ degrees are considered. Equation 3.16 is then updated as follows:

$$C(\omega_k, \theta_d) = \frac{\sum_{n=1}^{10} S_n(\omega_k) V_n^*(\omega_k, \theta_d)}{\sqrt{\sum_{n=1}^{10} |S_n(\omega_k)|^2 \cdot \sum_{n=1}^{10} |V_n^*(\omega_k, \theta_d)|^2}} \tag{3.18}$$

where ω_k represents the frequency component of the kth bin of the FFT where $(k = 0, 1, 2 \ldots N-1)$, and θ_d corresponds to a particular DOA such that:

$$\theta_d = \delta d \tag{3.19}$$

where $d = 0, 1, 2 \ldots (\frac{360}{\delta} - 1)^\circ$.

3.5.2 DF Antenna Characterisation

To characterise the DF antenna, a signal generator is connected to a transmitter which transmits a continuous sinusoid at the appropriate frequency at 0 degrees. The antenna characterisation table is then obtained by physically rotating the antenna in intervals of δ degrees from $0^\circ - 356^\circ$. The complex pairwise quantities are recorded for all apertures at each DOA and are stored in the table before rotating the antenna to the next DOA. At the end of a complete rotation of the antenna, the signal generator is tuned to a new frequency, and the procedure is repeated to generate a new characterisation table. It will be shown

later, that in practice a new table need not be generated for each new frequency depending on the fractional change in frequency.

The characterisation procedure is depicted below in Figure 3.12 where the antenna can be seen rotating in intervals of δ.

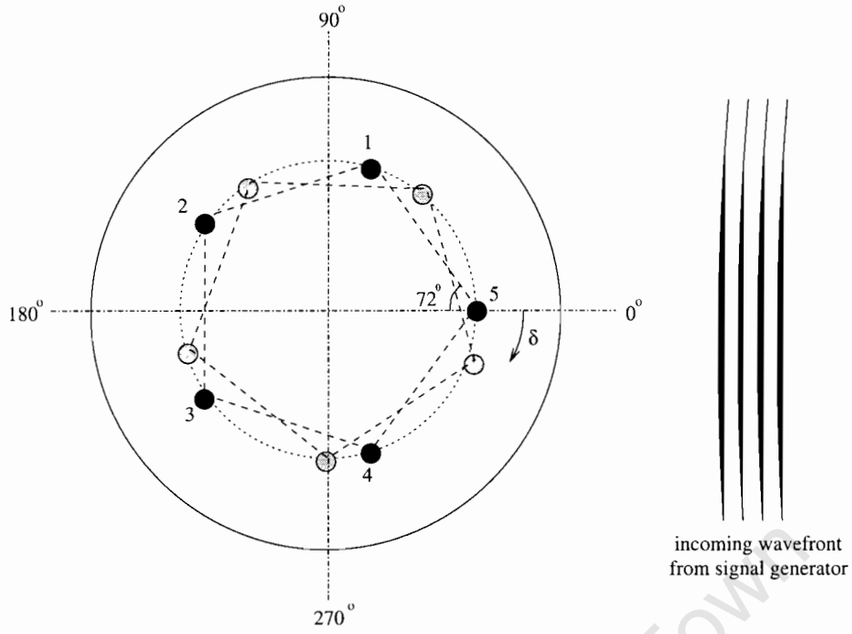


Figure 3.12: Characterisation of DF Antenna

3.5.3 Characterisation Table Inspection

The procedure for obtaining the characterisation table has been presented and discussed. This subsection is an investigation into the properties of the characterisation table. Both phase and amplitude properties are investigated and discussed for both a simulated characterisation table, and a real characterisation table generated using the 5 element DF array discussed earlier and a continuous wave signal generator.

Simulated Characterisation Table

Let us consider the structure for a single characterisation table generated at 903 MHz using the DF antenna (with the same element spacings depicted in Figure 3.2). Because the elements are closely spaced it would seem reasonable to assume that the signals on each of the antenna elements have unit amplitude. Consider aperture a_1 , i.e. element numbers (1,4) . We can see from Figure 3.12 that for an incoming wavefront at $0°$, the corresponding phase difference for this aperture is also $0°$. Maximal phase difference occurs after the antenna has been rotated through $90°$ as expected. The phase information in the correla-

tion table for this aperture (and all other apertures) is expected to vary sinusoidally with θ (c.f. Equation 3.6). The phase for the remaining apertures should be shifted replicas of a_1 offset by multiples of $72°$ depending on their positions relative to that of a_1. For example, if the phase of the correlation table for apertures a_1 and a_6 (lagging a_1 by $72°$) is plotted over θ, the variation in phase over DOA is observed in Figure 3.13.

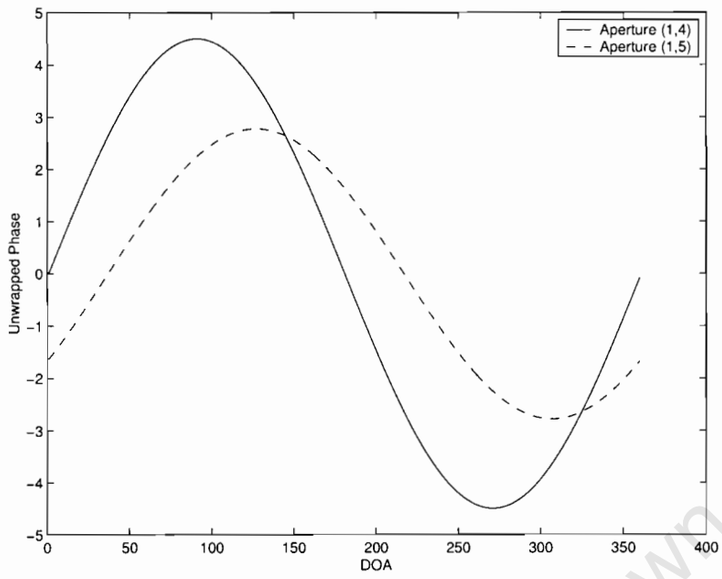


Figure 3.13: $\phi_n(2\pi 903\,MHz, \theta)$ for $DOA = 0° - 356°$ for apertures a_1 and a_6 of a simulated characterisation table

The reason aperture a_1 has a greater phase difference range than aperture a_6, is because the antenna elements are spaced further apart for aperture a_1 than those of aperture a_6.

Real Characterisation Table

In practice the phase of characterisation table is not purely sinusoidal. Due to the fact that the phase differences are calculated by performing a complex multiplication of the signals captured on the antenna elements, the effects of shadowing can affect the aperture phase information.

The characterisation table was generated by mounting the DF antenna onto a stepper motor which was then rotated in $4°$ steps. A continuous signal generator was tuned to 903 MHz (arithmetic mean of the uplink band) and placed at $DOA = 0°$ for the characterisation. The starting position and antenna element numbers were redefined as shown in Figure 3.14. Although these differ from the element positions that were previously defined, the characterisation allows for *any* DOA to be referenced to zero degrees depending on where the transmitter source is positioned at the start of characterisation.

Inspection of the recorded amplitudes for each of the antenna elements over θ yields the

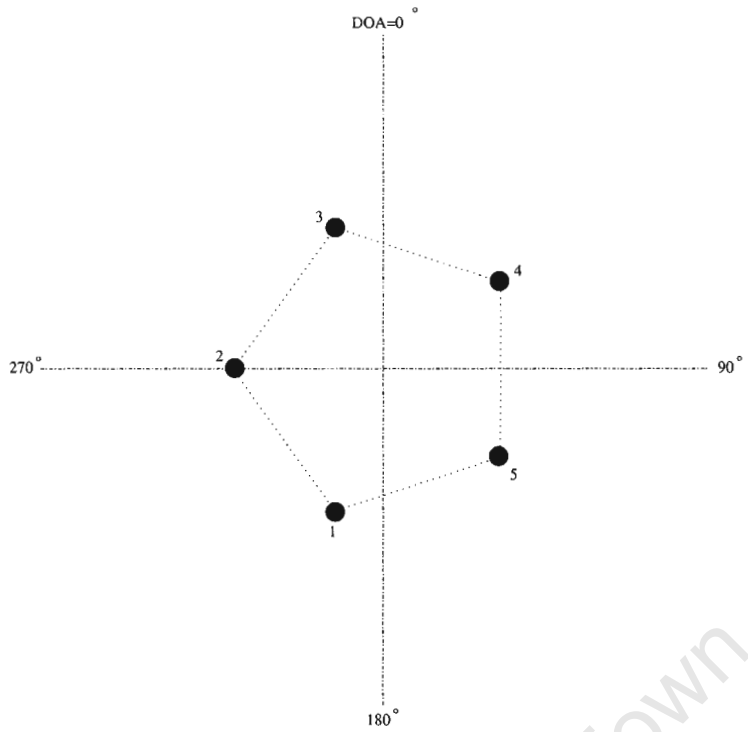


Figure 3.14: Antenna Element Positions for Real Data Recordings

following in Figure 3.15.

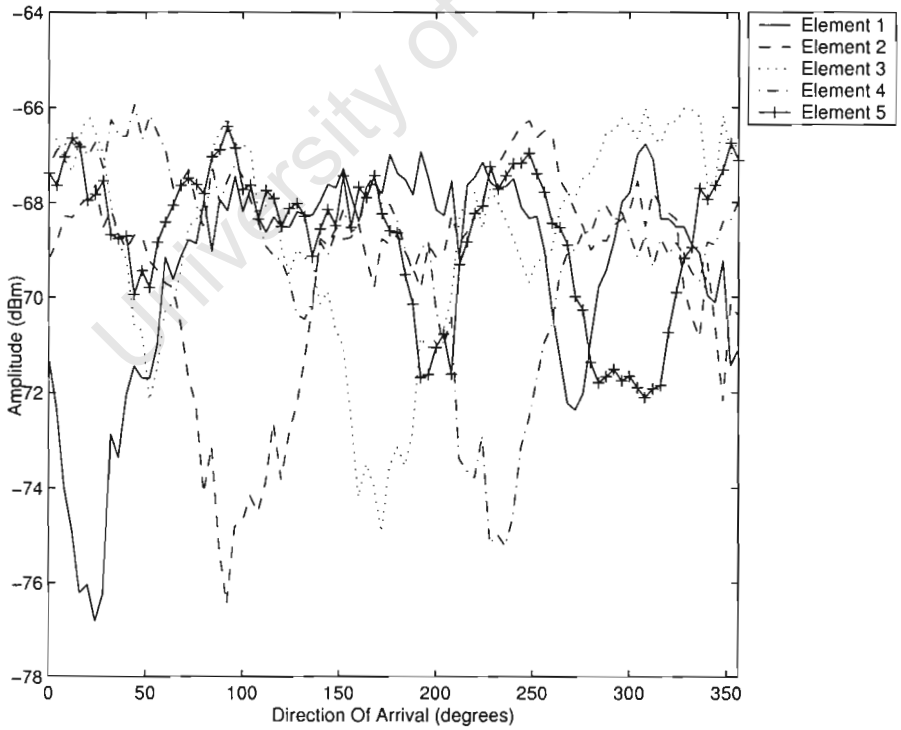


Figure 3.15: Antenna Element Amplitude Variation vs. DOA

We can see from the plot that the amplitude certainly does vary as a function of angle. Because the definition of the characterisation table is a combination of the element ampli-

tudes, it would be useful to investigate both the pairwise amplitude product and the phase differences. Because displaying the phase differences for the 10 apertures tends to somewhat clutter the plot, only two of the apertures are considered, namely a_{10} (elements 5,4) and a_1 (elements 1,4) . Both the phase, and the element products for the two apertures are shown in Figure 3.16 and Figure 3.17.

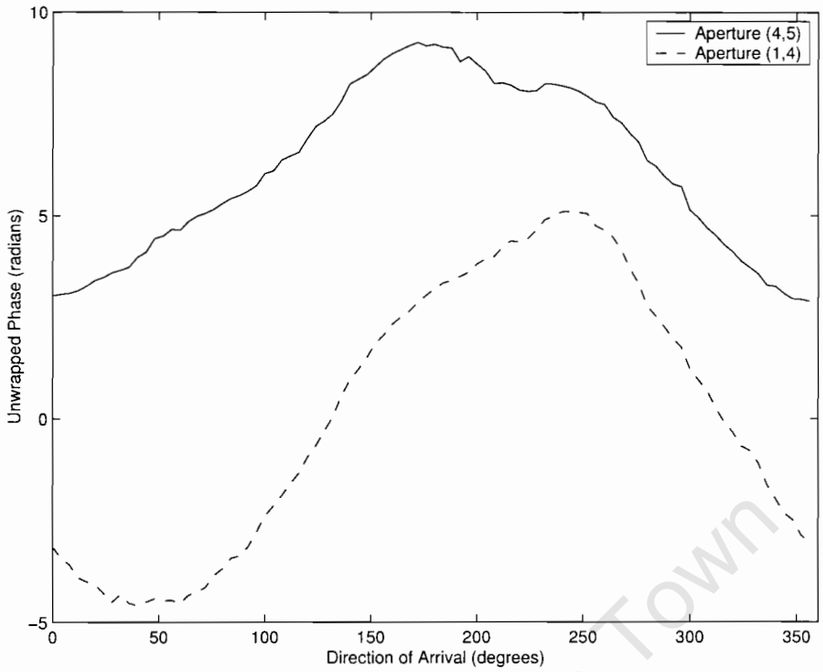


Figure 3.16: Unwrapped $\phi_n(2\pi 903\,MHz, \theta)$ for $DOA = 0° - 360°$ for apertures a_{10} and a_1 of a real characterisation table

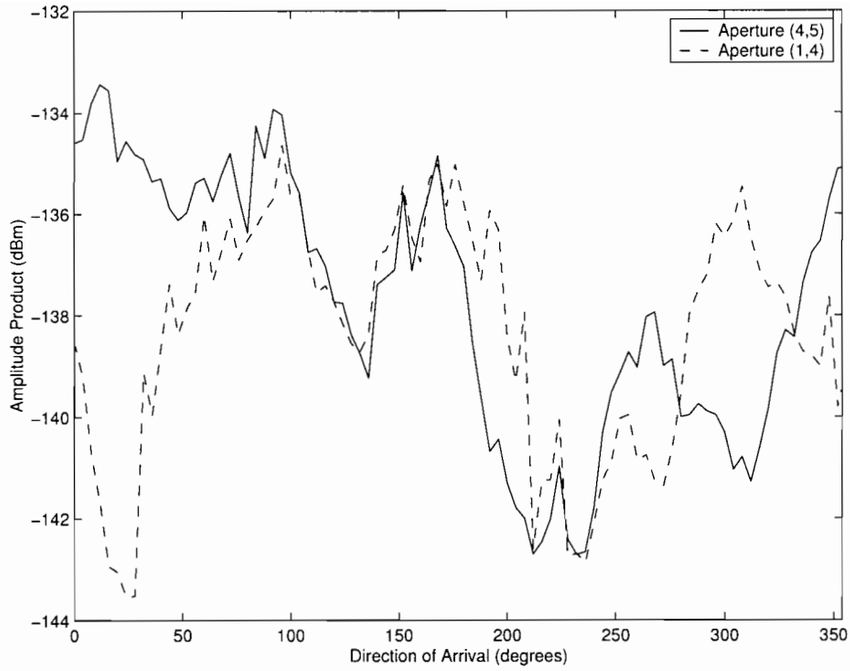


Figure 3.17: $|V_n(2\pi 903\,MHz, \theta)|$ for $DOA = 0° - 360°$ for apertures a_{10} and a_1 of a real characterisation table

If we observe Figure 3.16, we can see that the two phase curves are approximately sinusoidal as we expected. We can also see that the amplitude product can vary by as much as 9 dB which justifies the need for a real characterisation table over a simulated table (where the effects of antenna shadowing would be difficult to model).

3.5.4 The Effect of Using A Single Correlation Table for DOA Estimation of GSM Uplink Band

Recall that the GSM uplink band (the band under investigation) is in the range $890 - 915$ MHz and that for perfect correlation to occur across this band, a new characterisation table must be generated to estimate the DOA for each frequency component of the captured signals. For a signal comprising an FFT vector spanning 800 bins, this would require 800 calibrations. One might argue that instead of performing these calibrations at each unique frequency, tables could be computed at intermediate frequencies. Signals lying within the band between characterised frequencies could make use of interpolated calibration values. However it would be preferable to perform one calibration, which could be used over the 25 MHz uplink band.

To investigate the worst case scenario frequency mismatch, the algorithm output (discussed in the following section) was inspected for a simulated characterisation table generated at 890 MHz (radius 12.5 cm), and a single sinusoid at 915 MHz for *all* directions

of arrival. The mean of the estimated DOA error was found to be approximately 0. θ was considered in 4° increments ($\delta = 4$) from 0° to 356° (90 intervals). Recall from Section 3.4.2, that a quality factor of 1 occurs for a perfect match. The mean quality factor error function e_q is defined as follows:

$$e_q = \frac{1}{90}\sum_{d=0}^{89} 1 - \max_{\theta_d}\{Q(2\pi 915MHz, \theta_d)\} \tag{3.20}$$

where, $\max_{\theta_d}\{Q(2\pi 915MHz, \theta_d)\}$ is the maximum computed quality factor for the DOA θ_d. The results are shown in Table 3.3.

Characterisation Table Frequency (MHz)	890
Incoming Wavefront Frequency (MHz)	915
Radial Spacing (cm)	12.5
Angle Error (degrees)	$\approx 0°$
Mean Quality Factor Error (%)	**0.268%**

Table 3.3: Characterisation Table Investigation Results

The averaged quality factor error is very small. What this means is that at DOAs for which there is a perfect match, the correlation coefficient will drop from a maximal value of 1 down to 0.9973 which implies that one characterisation table is sufficient for the dataset acquisition in the uplink band.

3.5.5 Correlation Coefficient Inspection

The details of characterisation have been presented and discussed. This section serves to inspect the real correlation coefficients defined in Equation 3.18. The 5 element DF antenna depicted in Figure 3.2 was simulated (elements on a 12.5 cm radius). All monopoles were assumed to have omni-directional gain of 1. The characterisation table was also simulated in increments of $\delta = 1$ for the purpose of illustration. An incoming wavefront at a single frequency, ω_c from a $DOA = 180°$ was simulated applied to the algorithm. Antenna shadowing was not modelled, and as a result, the signals on each of the elements have unit amplitude.

The real part of the correlation coefficients, $Q(\omega_c, \theta)$ were then computed and plotted. A typical plot is illustrated in Figure 3.18.

As can be seen from the diagram, the dominant peak indicates the DOA. With a quality factor of 1, the peak can be seen to correctly correspond to a DOA of 180°.

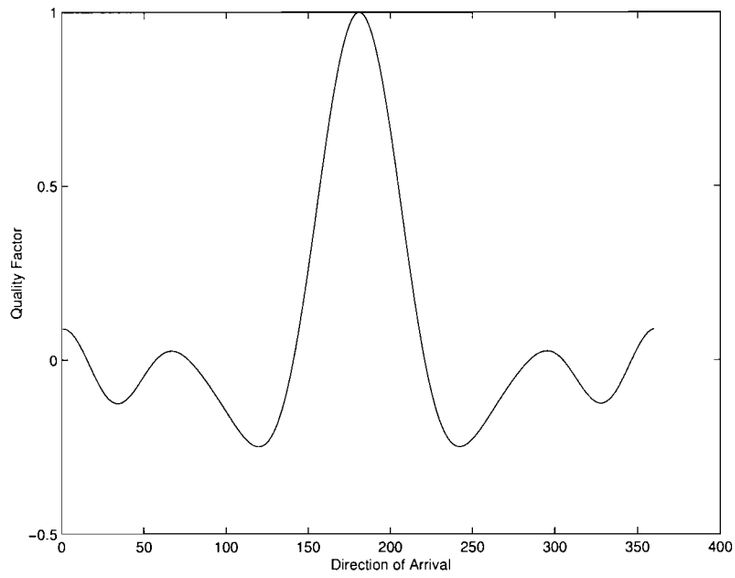


Figure 3.18: $Q(\omega_c, \theta)$ for an incoming wavefront at $180°$.

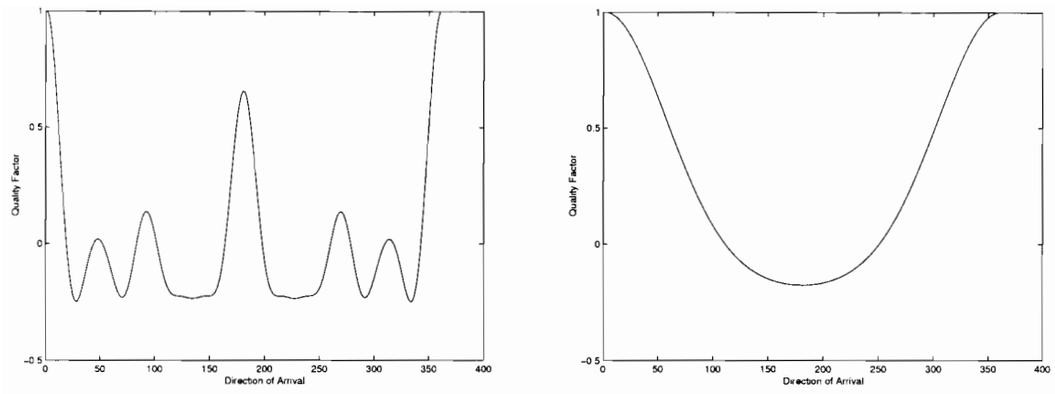
Depending on the correlation table spacing (δ), it is possible for the true DOA to not lie directly on the maximum peak of curve. For example, if $\delta = 4$ and the true DOA for an incoming wavefront is at $6°$, the true DOA will lie between sample points at $DOA = 4°$and $DOA = 8°$. To determine the true DOA, the maximum quality factor value is found and its corresponding DOA is determined. A quadratic is then fitted through the peak and neighbouring points on either side of the peak, and the true DOA is given where the fitted quadratic attains a maximum.

Before launching into an evaluation of the algorithm when applied to GMSK signals, it would be useful to try to explain the shape of the plot, paying special attention to the peaks of the correlation coefficients and how the DF antenna geometry actually affects the DOA estimate.

3.6 Antenna Element Spacing Investigation

If we inspect Figure 3.18 carefully, we notice that there are secondary peaks about the main peak at $DOA = 60°$ and $DOA = 300°$ and a third at $0°$. These secondary peaks can lead to erroneous DOA predictions as situations may arise where they dominate the true peak in the presence of additive noise. The severity of the secondary peaks can be controlled by adjusting the spacing of the elements.

As mentioned earlier, for unambiguous DOA estimation for a simple two element DF array, antenna pairs should be spaced less than half a wavelength apart. However for a DF antenna comprising several elements, this requirement can be relaxed as there are



(a) r = 26.8cm (b) r = 5.2cm

Figure 3.19: The Effect of Adjusting the Element Spacing

always other antenna pairs whose phase differences at particular DOAs are less than half a wavelength.

At a frequency of 900 MHz, the corresponding wavelength in free space is approximately 33.3 cm. Because the elements are on a radius of 12.5 cm, the spacing between adjacent elements (pentagon apertures) is approximately 7.7 cm but the spacing between opposite elements (pentagram apertures) is 23.8 cm which is greater than half a wavelength.

Before motivating the radial choice of 12.5 cm, let us consider 2 cases as follows in which the spacing between elements is adjusted as follows:

1. The element spacing for *pentagon* apertures is slightly less than half a wavelength.
2. The element spacing between *pentagram* apertures is slightly less than half a wavelength.

Using simple trigonometry, the corresponding radii for cases 1 and 2 was found to be 23.8 cm and 5.2 cm respectively. Let us consider a wavefront at $DOA = 0°$. The output of the DOA algorithm ($Q(900MHz, \theta)$ for cases one and two is shown in Figure 3.19.

If we inspect both plots carefully, we can see that the DOA is correctly given at $0°$. However, in the first case, there are a few unambiguous peaks, the most significant occurring at $180°$. The amplitudes of these peaks increase as the elements are spread further apart. The peaks in the first case are due to the fact that the pentagram apertures are more than half a wavelength apart. One advantage though of having them further apart, is that the width of the main lobe is narrower, making it easier to identify the correct DOA.

Although the second case looks more attractive (no phase ambiguities), the dynamic range of the phase differences between adjacent elements (pentagon apertures) is much less than it would be if the elements were spaced slightly less than half a wavelength apart. This

makes the DOA estimation more sensitive to the effects of noise. Noise would tend to amplify phase ambiguities in the first case, whereas the DOA peak in the second case will tend to be shifted.

3.6.1 Worst Case Antenna Element Radius Investigation

We have seen thus far, that the output of the DF algorithm varies as the element radius is altered. It would be interesting to investigate whether there is an optimal radius for estimating the DOAs for GSM signals. The choice of 12.5 cm arose as a tradeoff between dynamic phase range, and phase ambiguity as the pentagon apertures are less than half a wavelength apart, and the pentagram apertures are greater than half a wavelength apart. In order to assess if this is a suitable choice, we have to have some way of measuring an erroneous DOA estimate. Let us define an error function as follows:

$$e_r = W\left(\theta_{true} - \theta_{est}\right) \tag{3.21}$$

where θ_{true} is the known a-priori DOA, θ_{est} is the corresponding estimated DOA, and $W(\theta_{true} - \theta_{est})$ is the wrapped angular difference of $(\theta_{true} - \theta_{est})$ i.e. $-180° \leq W(\theta_{true} - \theta_{est}) < 180°$. The wrapping of the angle difference is necessary, so that in a worst case scenario of $\theta_{true} = 0°$ and $\theta_{est} = 359°$, the error function is produces $e_r = -1°$ rather than $e_r = -359°$ which would be incorrect.

Three Monti Carlo simulations were run in MATLAB at signal to noise ratios of 30, 20 and 10 dB respectively to investigate the effect of varying the radius on the performance of the DF algorithm. For each of these SNRs, 500 000 iterations were performed for each radial increment *over* the range: $0.01m \leq r \leq 0.35m$ in 5mm increments. A wavefront at $DOA = 18°$ (arbitrarily chosen, although all angles yield similar results) at a frequency of 903 MHz (approximate arithmetic mean of the uplink band) was simulated for *each* radial increment. As the radius was increased, a new *ideal* characterisation table was generated accordingly.

The results for SNRs of 30, 20 and 10dB are shown below in Figures 3.20, 3.21 and 3.22 which show a plot of the standard deviation of the error function (in degrees) vs. the circular radius.

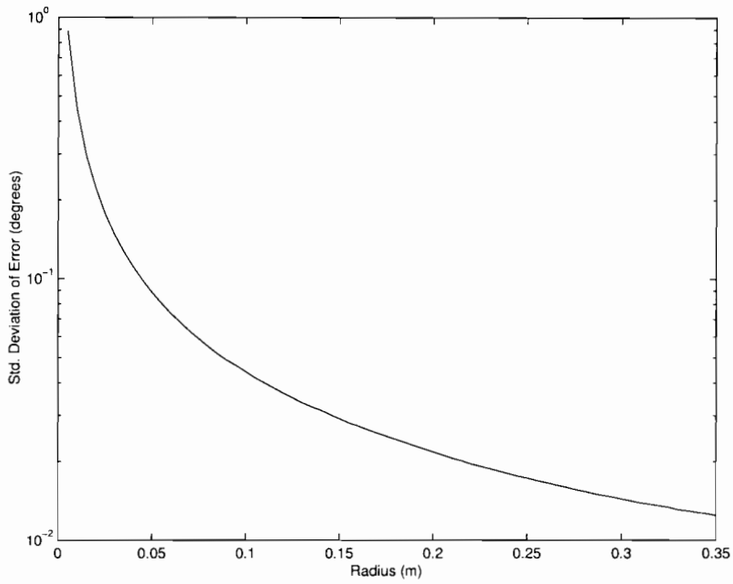


Figure 3.20: Standard Deviation of the Error Function for SNR = 30dB

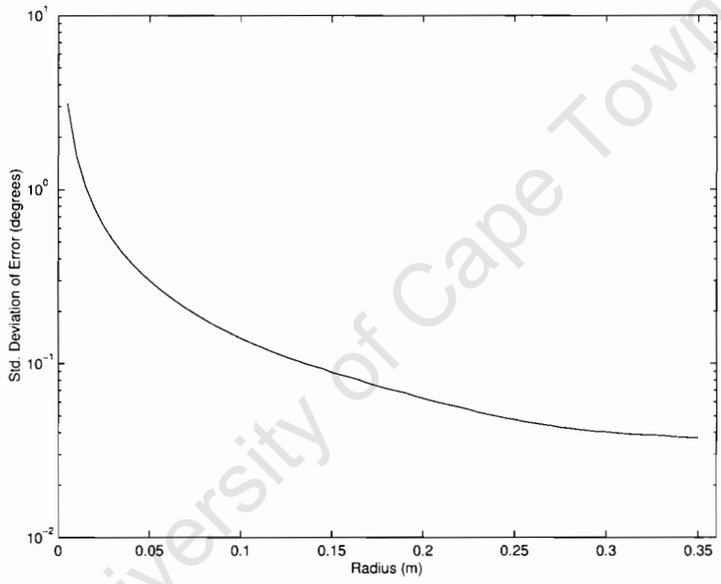


Figure 3.21: Standard Deviation of the Error Function for SNR = 20dB

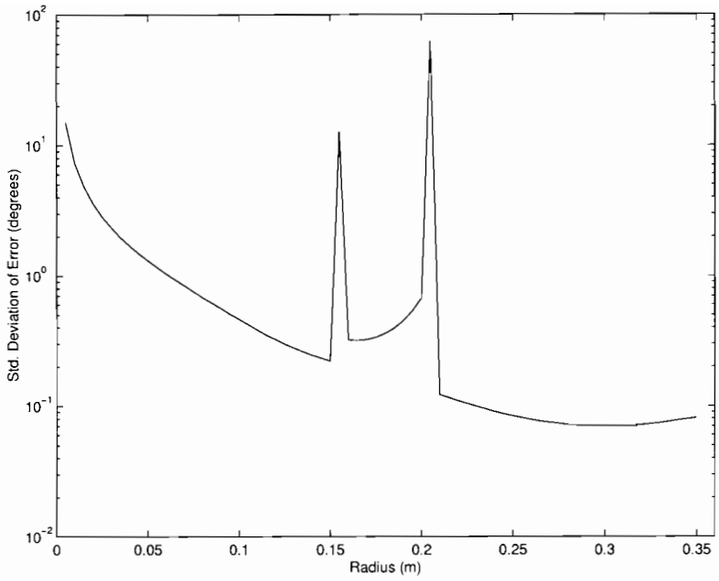
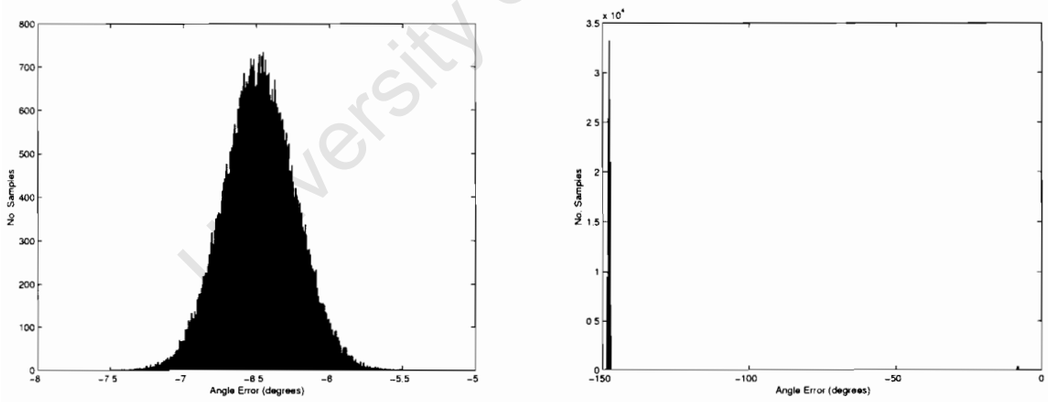


Figure 3.22: Standard Deviation of the Error Function for SNR = 10dB

It is interesting to note that at radii $r = 15.5\,cm$ and $r = 20.5\,cm$, the DOA correlative algorithm breaks down resulting in angular ambiguities. At $r = 15.5\,cm$, the element spacing between pentagon apertures corresponds to $l_{pentagon} = 14.69\,cm$ which is approaching half a wavelength at 903 MHz ($\lambda = 16.6\,cm$). It should be noted that the spacing between pentagram apertures at $r = 15.5\,cm$ is $l_{pentagram} = 29.48\,cm$ which is significantly greater than half a wavelength. The phase ambiguity is more clearly observed if histograms of the error function are observed at $r = 14\,cm$ and $r = 15.5\,cm$. These are shown in Figure 3.23.



(a) r=14 cm

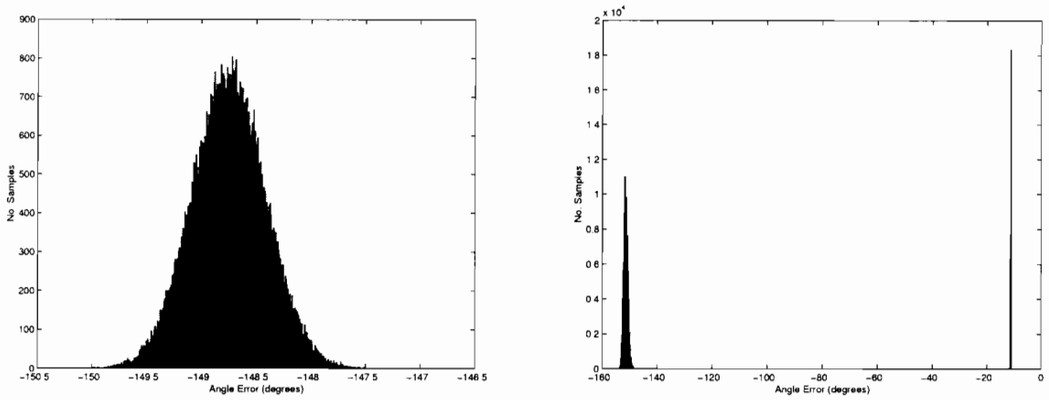
(b) r=15.5 cm

Figure 3.23: Histogram of Error Function for SNR=10dB

As the radius is increased to $r = 15.5\,cm$, the angle error increases significantly to almost $-150°$. The original error of only $-6.5°$ is still present, but is far less prevalent. The reason

for the occurence of the greater DOA error when $r = 15.5\,cm$, is because a secondary peak has exceeded the quality factor of the true peak resulting in an erroneous DOA.

At a radii of $15.5\,cm \leq r \leq 20.5\,cm$, we observe that the angular error has become even worse, and that the mean of the error, rather than being at $0°$ (ideally) is at $-148.75°$.



(a) r=17.5 cm

(b) r=20.5 cm

Figure 3.24: Histogram of Error Function for SNR=10dB

A final interesting plot to observe, is that of the *mean* of the error function in degrees as a function of radius. This more clearly illustrates the radii at which the DF technique breaks down particularly in low SNR environments. The mean of the error function in 30, 20 and 10dB SNRs are shown in Figures 3.25, 3.26 and 3.27 respectively.

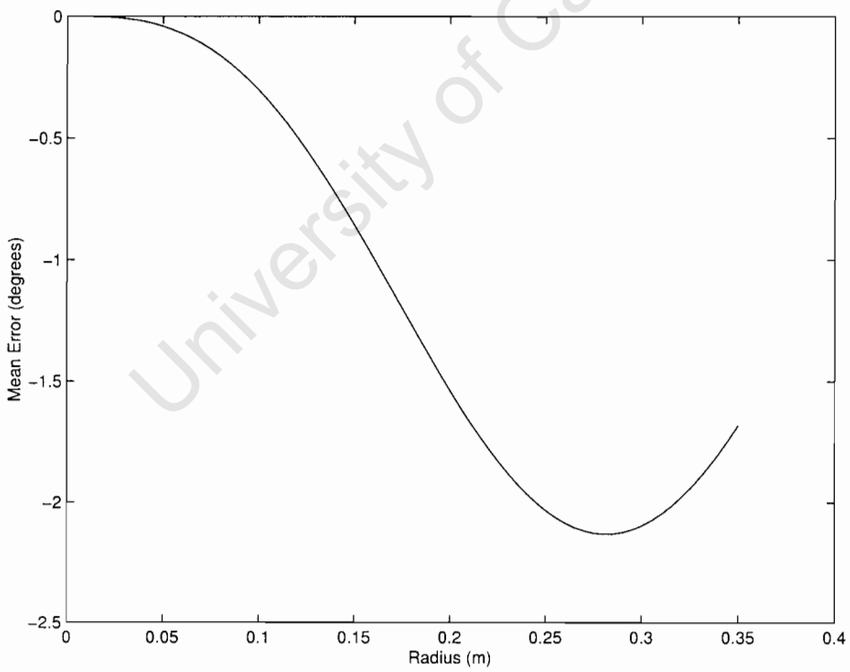


Figure 3.25: Mean of Error Function for SNR = 30dB

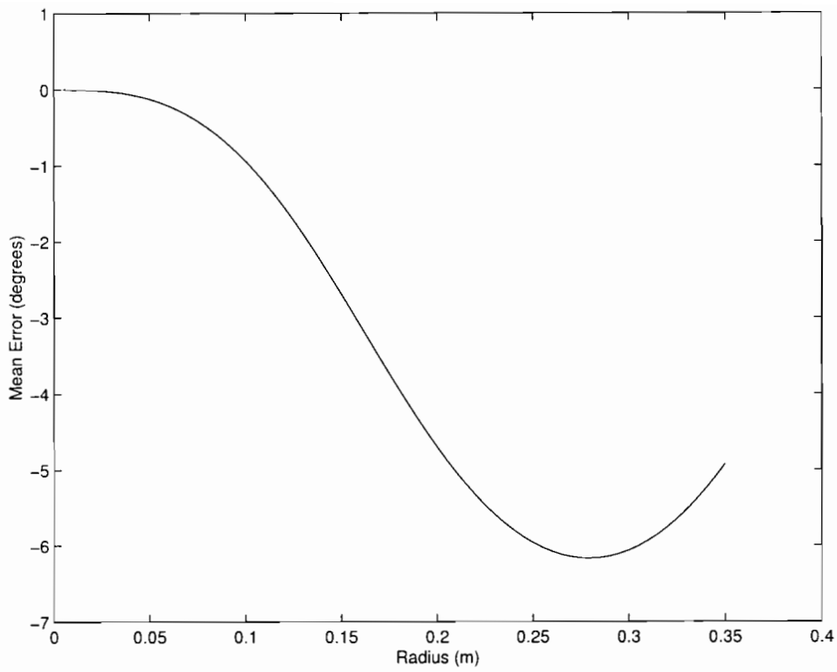


Figure 3.26: Mean of Error Function for SNR=20dB

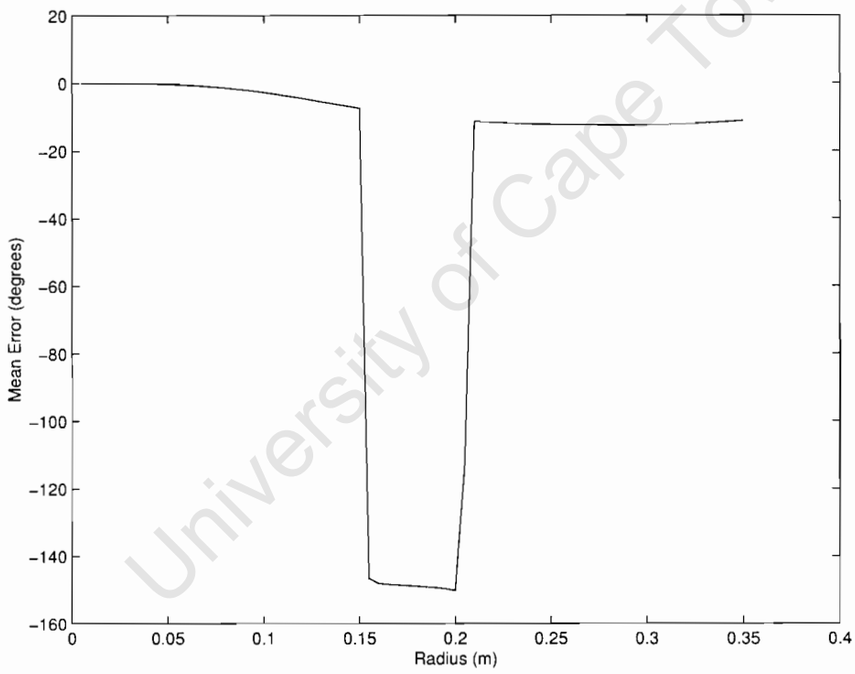


Figure 3.27: Mean of Error Function for SNR=10dB

After assessing both the mean and the standard deviation of the error function plots in low signal to noise ratio environments, it would seem that the chosen radius of $r = 12.5cm$ presents a good choice for the tradeoff between the angular error vs. the standard de-

viation of that error. Although the plots depicted are for one DOA only, similar results were observed for other DOAs. It is very difficult to quantify accurately whether this investigation would yield similar results if a real characterisation table had been used for each radial increment (rather than a simulated one) as each characterisation table would differ for each unique radius. A further complication, is that as the radius is increased, the effect of shadowing is reduced. This means that the "null" points due to shadowing in Figure 3.17 would shift, making the SNR on each element at each DOA for each radius unique. A more accurate study would have to be performed by obtaining real characterisation tables at each radius, and then investigating the standard deviation of error function for each radius at DOAs where nulls occur in the amplitude plots similar to Figure 3.17.

3.7 DOA Investigation of GMSK Signals

The correlation coefficients for a modulated carrier were inspected in Section 3.5.5. This section serves to illustrate the correlation coefficients for a basebanded analytic GMSK signal, followed by multiple GMSK signals. An appropriate signal model will be described in the next chapter when the GSM simulator is discussed. For now, the purpose of this section is merely to illustrate the output of the correlation coefficients produced by the correlative DOA algorithm.

3.7.1 DOA Estimation of a Single GMSK Waveform

A basebanded analytic signal, $x(t) = Ae^{j(\phi(t)+\phi_0)}$ was simulated at 890 MHz at a DOA of 45° to the DF antenna. The magnitude of the FFT of the windowed signal is illustrated in Figure 3.28.

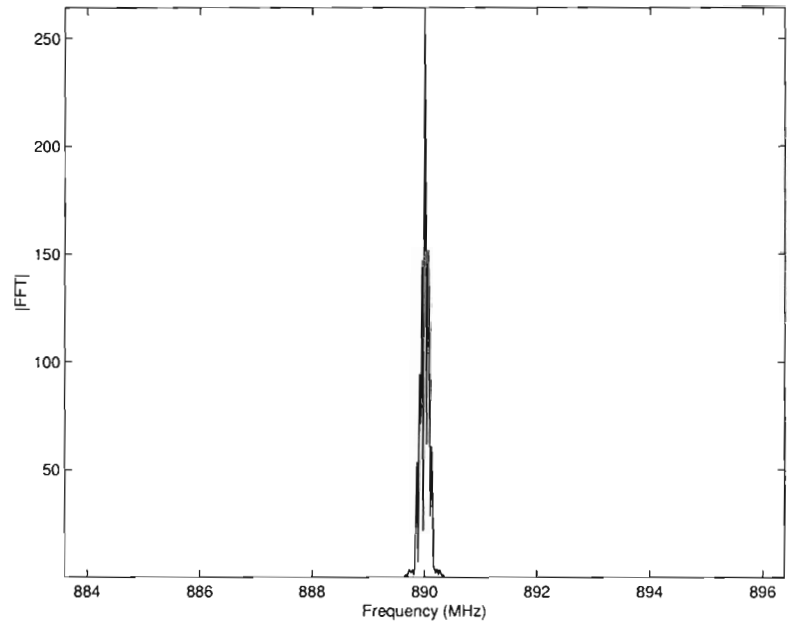


Figure 3.28: |FFT| for a GMSK Signal at 890 MHz

The output of the DOA algorithm yields the correlation coefficients, the real part of which is illustrated in Figure 3.29. No Gaussian noise was added to the datasets before computing the correlation coefficients.

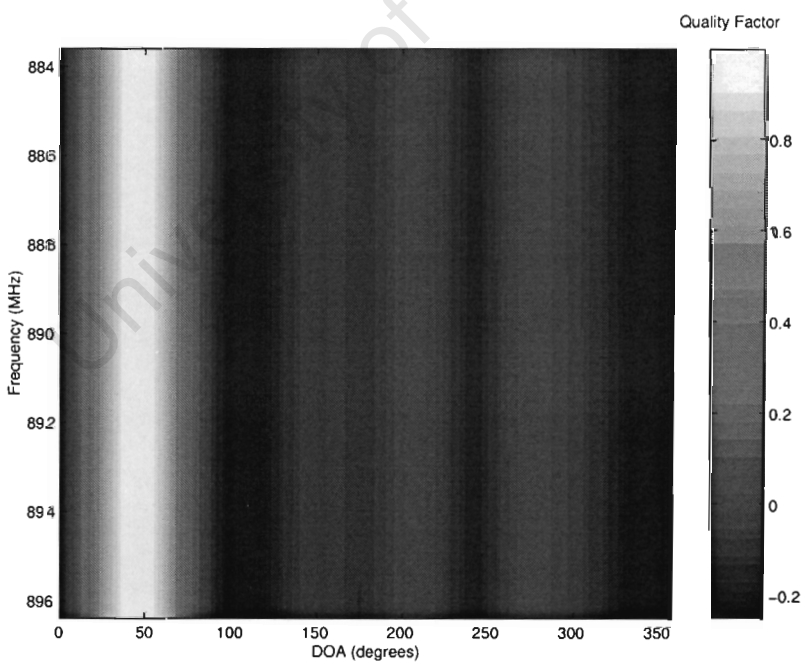


Figure 3.29: $Q(\omega, \theta)$ in Noise Free Environment for incoming wavefront at $45°$

One can clearly see the predicted DOA of $45°$ across **all** frequency bands even though the GMSK signal is centred at 890 MHz and is tightly bandlimited to 200 kHz. The reason for this is because the premature time domain truncation of the GMSK signal (due to the 80 μs capture window) produces spillage into bins across the frequency band (c.f.

Section 3.3.2). Because there is no noise being added to the signal in this simulation, the phase difference for all frequencies in the band of interest is constant, and thus yields a quality factor of 1 across the entire band.

Addition of Bandlimited Gaussian White Noise

If we add bandlimited Gaussian white noise to the datasets before computing the correlation coefficients, we observe $Q(\omega, \theta)$ in a SNR environment of 20 dB in Figure 3.30.

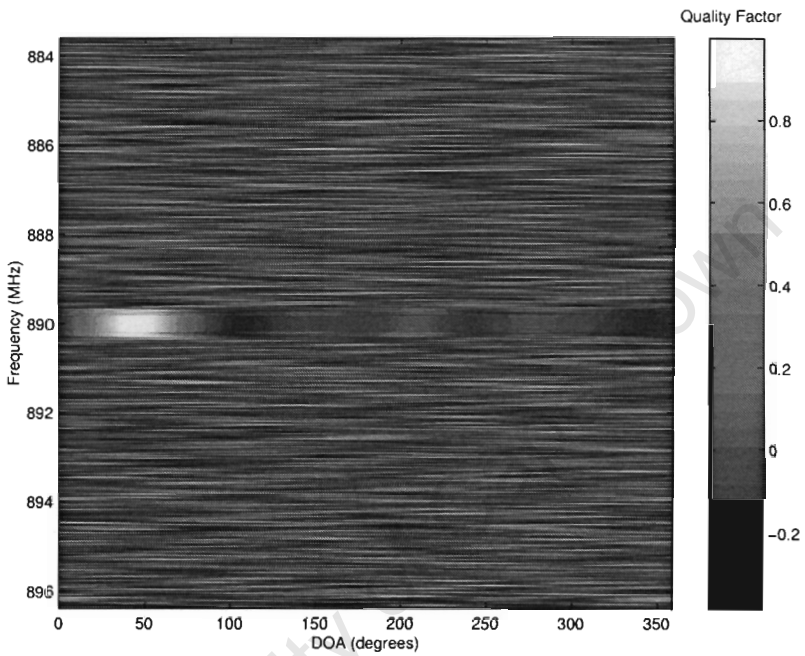


Figure 3.30: $Q(\omega, \theta)$ for incoming wavefront at 45°in SNR = 20 dB

As we can see across the width of the main lobe of the GMSK signal, the quality factor is relatively constant attaining a maximum at the peak of the main lobe at a $DOA = 45°$.

3.7.2 DOA Estimation of Multiple GMSK Signals

Up to now, the DOA estimation of a *single* GMSK signal has been considered. What happens if there are two or more signals in the band of investigation? The resultant signal present on the DF antenna at the sampling instant is given by the sum of the N signals impinging on the antenna:

$$\overrightarrow{S} = \sum_{i=1}^{N} \overrightarrow{s_i} \tag{3.22}$$

$$= \sum_{i=1}^{N} A_i e^{j\phi_i} \tag{3.23}$$

$$= \sum_{i=1}^{N} A_i e^{j2\pi\left(\frac{R_i}{\lambda_i}\right)} \tag{3.24}$$

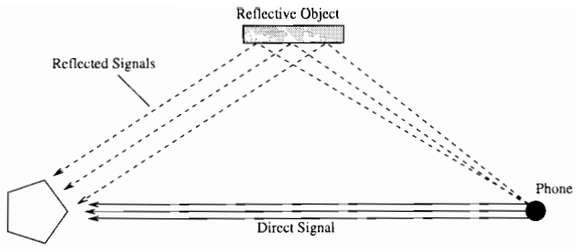
where R_i and λ_i are the distance from the DF antenna and the wavelength of the ith signal.

Two Wavefronts of Identical Wavelengths

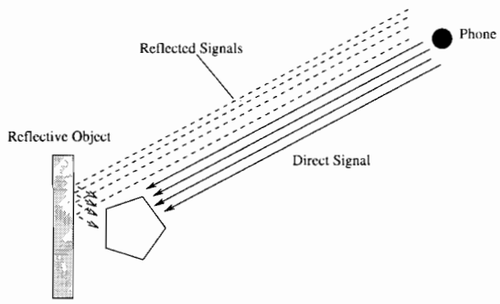
The instantaneous phases and wavelengths for the several wavefronts can have a varying effect on the DOA algorithm, leading to erroneous DOA estimation in cases where the wavelengths are identical.

While the GSM standard does not allow two mobile users in the same cell to occupy the same time/frequency slot simultaneously, it is possible however for two users to make use of the same frequency carrier, but reside in adjacent time slots. The information from both users can potentially overlap at the DF antenna depending on their positions relative to the serving base station and DF antenna. This is covered in the thesis in more detail later.

Another situation in which frequency overlap may arise is due to multipath. Depending on where the handset is located (in a building for example), several reflected signals may impinge on the DF antenna simultaneously. If reflective objects are far from the antenna, this should not present too much of an issue as the power in the reflected signals is likely to be much weaker than that of the direct line of sight signal. However, if the DF antenna is in close proximity to a reflective object, the signal strength of the reflected signals on the DF antenna would more likely resemble the signal strength of the direct signal leading to erroneous DOA estimation. This is illustrated in Figure 3.31.



(a) Distant Reflective Object



(b) Close Proximity Reflective Object

Figure 3.31: Multipath Scenarios

The effects of these two situations may be investigated by simulating two *identical* GMSK signals both at 903 MHz, but at slightly different distances from the DF antenna approaching at two different angles. The geometry is illustrated in Figure 3.32.

Two phones are placed in the scene at distances $L\lambda$ and $(L + d)\lambda$ from the DF antenna. L was arbitrarily chosen such that the DF antenna is in the far field region and $0 \leq d < 1$ i.e. phone 2 is moved in fractions of a wavelength from the DF antenna relative to phone 1.

If phone 1 and phone 2 are exactly the same distance from the DF antenna, transmitting identical signals with equal signal powers, intuitively we might expect the DOA algorithm to predict some sort of averaged DOA at $45°$. This is not the case however and depends on what fraction of a wavelength the second source is relative to the first (assuming the phase functions and powers for the two transmitters are identical). The quality factors are illustrated in Figure 3.33.

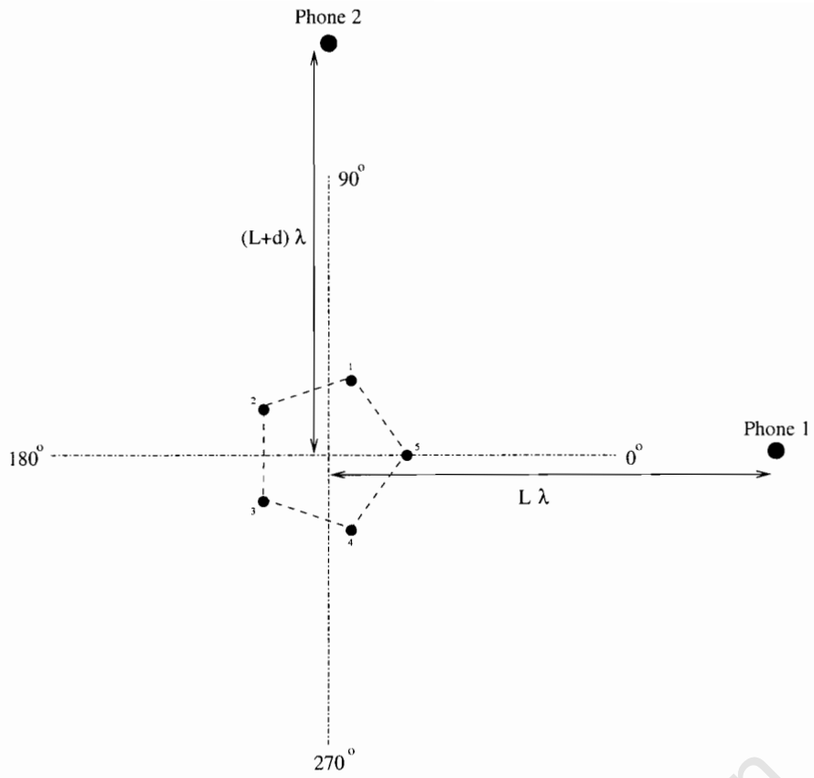


Figure 3.32: Placement of two phones in a scene

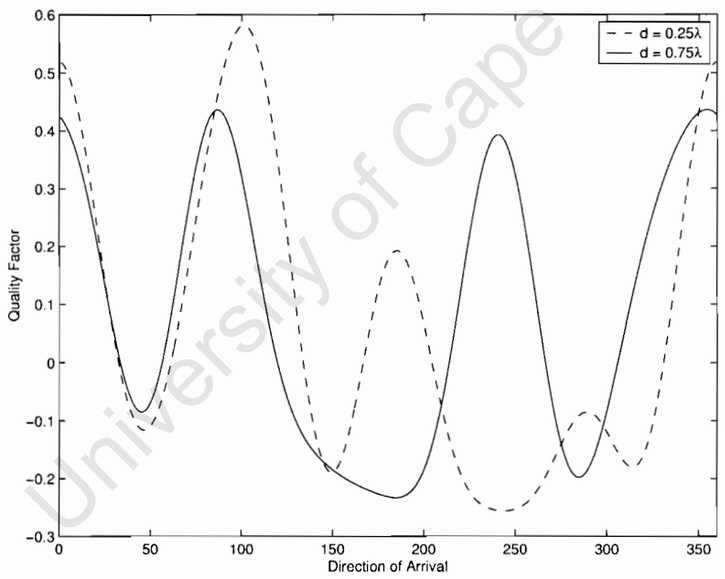


Figure 3.33: Effect of altering distances d from DF antenna by fractions of a wavelength

A clearly defined DOA cannot clearly be observed for either of the two values of d. The erroneous DOA is more severe when $d = 0.75$ as the quality factors for the peaks are very similar and in the presence of noise may yield a $DOA \approx 250°$.

To further illustrate this, consider two signals s_1 and s_2 arriving at the antenna from 0° and 180°. One would expect a DOA estimation of either 90° or 270°. However, the phase difference between element combinations 1,4 and 2,3 would be 0° for $DOA = 0°$ and $DOA = 180°$ (the wavefront is perpendicular to the aperture), whereas for a signal approaching from 90° or 270°, maximal phase difference would be observed between the elements of the two combinations.

We can conclude from this that it really depends on the resultant phase measured on the five antenna elements before the correlation coefficients are computed. In some cases, destructive or constructive interference may arise, depending on the instantaneous phases and powers of the various incoming wavefronts. This leads to an indeterminable number of different DOAs.

In order to estimate the directions of arrival for more than one incoming signal at identical frequencies, subspace-based methods such as MUSIC and ESPRIT or parametric methods should be explored. Krim and Viberg present a good introduction on subspace and parametric methods for additional interest [5].

Two Wavefronts of Differing Wavelengths

The output of the DOA algorithm for incoming wavefronts of differing wavelengths was investigated. Two wavefronts at frequencies of 898 and 903 MHz were simulated at $DOA = 45°$ and $DOA = 180°$. The SNR was set at 20 dB. The resulting correlation coefficients are shown below in Figure 3.34.

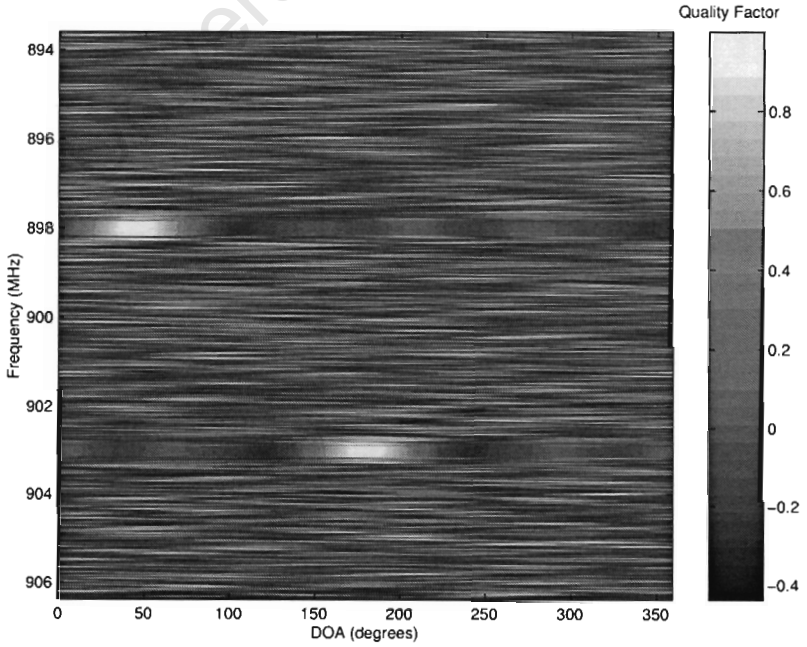


Figure 3.34: $Q(\omega, \theta)$ for two Incoming Wavefronts at $DOA = 45°$ and $DOA = 180°$ for SNR = 20 dB

The DOAs can clearly be seen for the two incoming wavefronts.

3.8 Incorporating GSM Specific Information to Improve DOA Estimation

We have seen how the correlation coefficients are produced by the DOA algorithm, and inspected the coefficients produced for GMSK signals in the previous section. If the algorithm could incorporate the GSM frequency information (in particular the known bandwidth of the GMSK signals, and the GSM carrier frequencies), better DOA estimates could be computed by averaging the aperture information over the GMSK band as the frequency content for a particular aperture should be virtually identical across the 200 kHz bandwidth of a GMSK transmission.

Recall from Section 3.4.2 that the aperture product, $S_n(\omega)$, is the complex product of the Fourier transforms of the signals captured on the antenna pair defining the nth aperture. We know a-priori from the GSM standard where the carriers reside (c.f. Section 2.3). For a discrete system, we can compute the frequency bins at which these carriers occur. Once this is known, the frequency information for each aperture can be averaged and substituted back into $S_n(\omega)$ across the 200 kHz bandwidth for each carrier. This averaging operation would improve the signal to noise ratio, and would result in a more certain DOA estimation for a particular carrier. Let us define the averaged aperture information across a 200 kHz wide GMSK waveform as:

$$\overline{S_n(\omega_c)} = \frac{1}{N} \sum_{l=-N/2}^{N/2} S_n(\omega_c + l\Delta\omega) \tag{3.25}$$

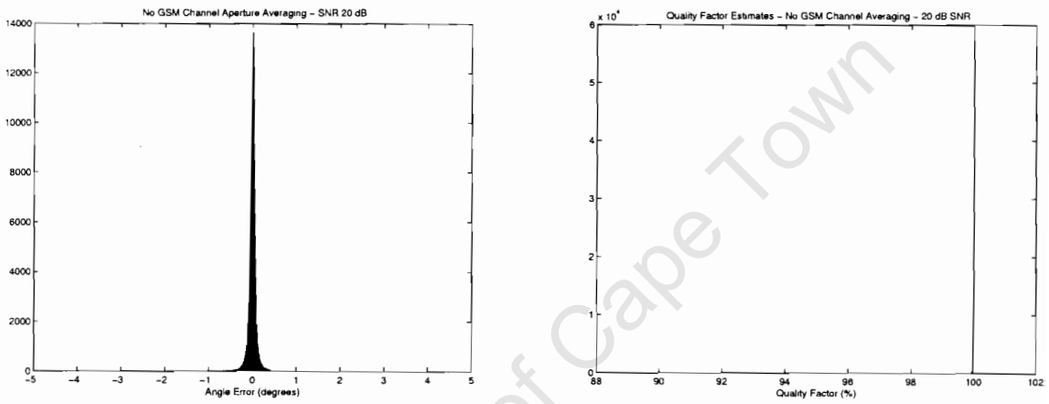
where ω_c represents the frequency at which a GSM carrier resides, and N represents the number of frequency samples occupied by the 200 kHz, given a certain FFT resolution $\Delta\omega$. Note that $N = \frac{2\pi 200e3}{\Delta\omega}$. Recall from Table 3.1, that for a capture window of $80\,\mu s$, the corresponding FFT resolution, $\Delta\omega = 2\pi 12.5\,kHz$ which means that $N = \frac{200}{12.5} = 16$.

To summarise, an average of the aperture information has been performed over each GSM carrier in $S_n(\omega)$. A simple average is possible (without incorporating a frequency phase shift to each frequency component in $S_n(\omega)$) because the fractional change in frequency relative to the GSM carrier is very small, which means that the phase values for components in the FFT around the carrier should be virtually identical.

3.8.1 Statistical Analysis on GMSK Signals

To investigate the effects of the carrier averaging operation, Monte Carlo simulations were run which involved a single phone at 0°to the DF antenna transmitting a GMSK signal. $80\,\mu s$ of data was simulated at a sample rate of 12.8 MHz, which yielded a 1024 point FFT. The apertures were constructed, and the direction estimates were computed for each of the frequency bins. The simulation was performed 20 000 times in varying signal to noise environments with randomly generated GMSK waveforms (the bit streams were randomly generated). Histograms of the direction errors (limited between $-5°$ and $5°$), and quality factors (limited between 80% and 100%) for the current DOA algorithm with no GSM carrier averaging are shown in Figures 3.35 3.36 and 3.37 for SNRs of 20 dB, 10 dB and 3 dB respectively.

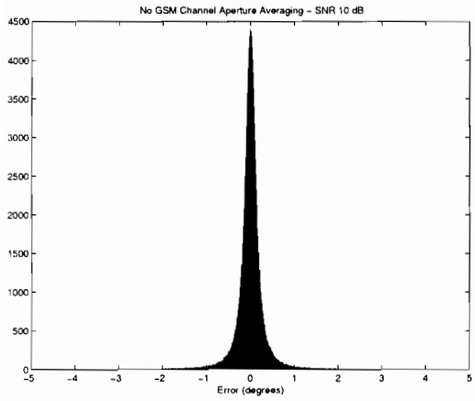
Effect of No GSM Carrier Averaging



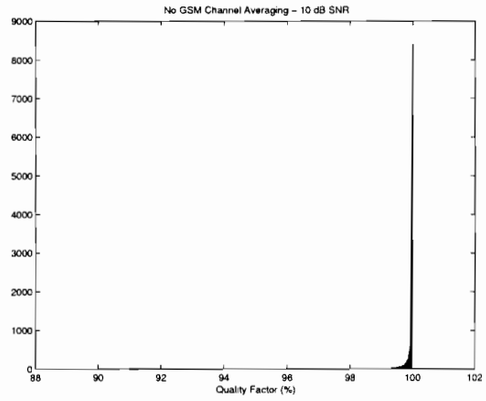
(a) Histogram of Direction Error

(b) Histogram of the Quality Factor

Figure 3.35: SNR 20 dB (no GSM carrier averaging)

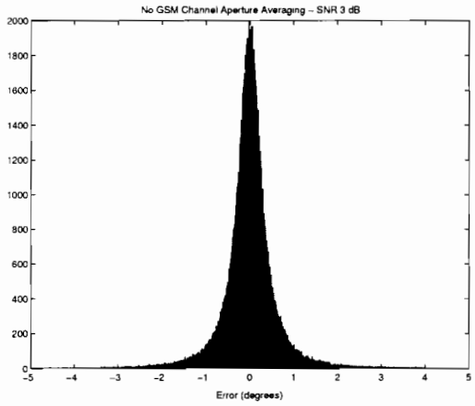


(a) Histogram of Direction Error

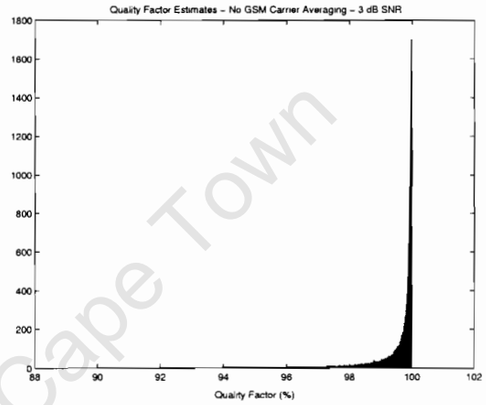


(b) Histogram of the Quality Factor

Figure 3.36: SNR 10 dB (no GSM carrier averaging)



(a) Histogram of Direction Error



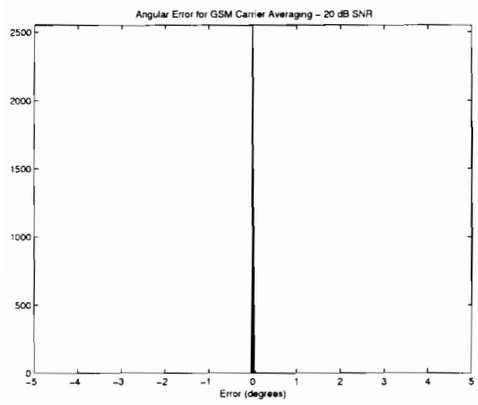
(b) Histogram of the Quality Factor

Figure 3.37: SNR 3 dB (no GSM carrier averaging)

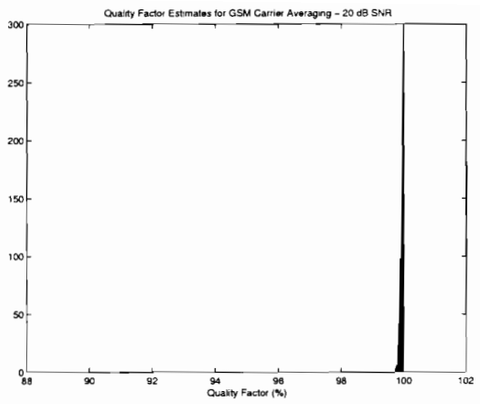
Looking at the three plots, one can clearly see that the both the quality factor and the direction estimates degrade rapidly as the SNR is reduced. The reader should observe the spread of the error function. Although it is not illustrated in the plots, some direction errors were seen to be out by as much as 180° and the quality factor was seen to drop as low as -25% in a SNR of 10 dB and below.

Results for GSM Channel Averaging

Let us now average the aperture information as discussed earlier. The simulation parameters were kept identical, and the histogram plots are shown in Figures 3.38, 3.39 and 3.40.

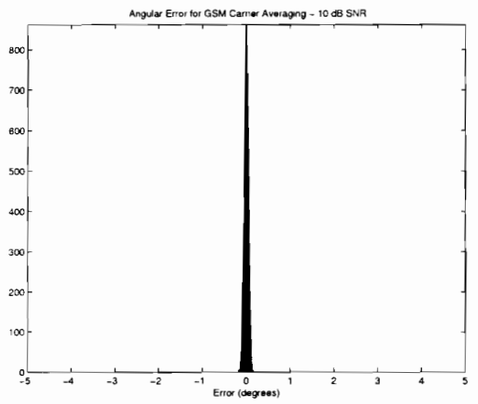


(a) Histogram of Direction Error

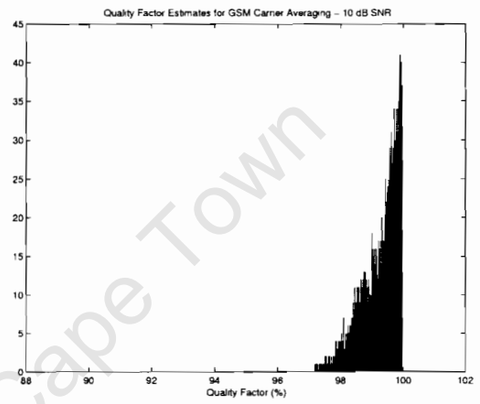


(b) Histogram of the Quality Factor

Figure 3.38: SNR 20 dB (GSM carrier averaging)

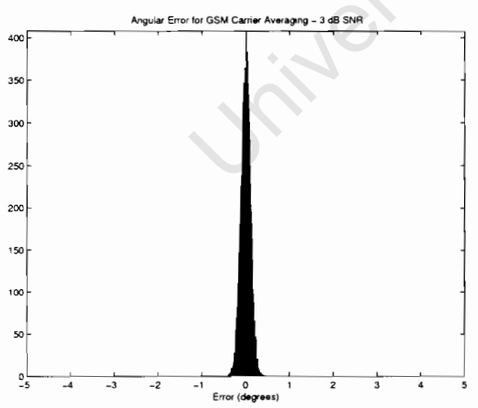


(a) Histogram of Direction Error

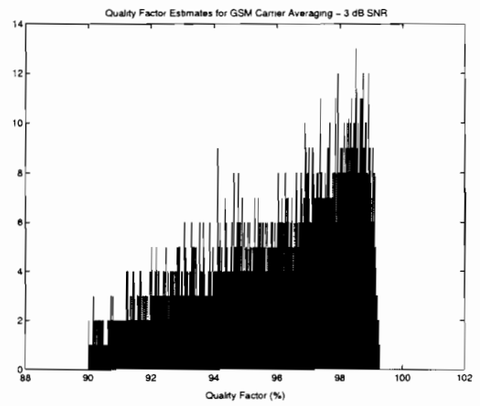


(b) Histogram of the Quality Factor

Figure 3.39: SNR 10 dB (GSM carrier averaging)



(a) Histogram of Direction Error



(b) Histogram of the Quality Factor

Figure 3.40: SNR 3 dB (GSM carrier averaging)

An improvement in the spread of the error function is observed as a result of the averaging operation. Consider a SNR of 10 dB. With no carrier averaging, although rare, some direction estimates may be out by as much as $180°$. With carrier averaging however, a maximal error of $0.2°$ was recorded. The quality factors are also more compact for the latter case.

Finally, if we inspect the quality factor histogram for the third plot (3 dB SNR), although the maximum quality factor of 100% is never attained, at first glance the quality factor plot for the non-averaged plot appears "better" than that of the averaged case. However, one should note that only quality factors between 90% and 100% were displayed in the histogram. The minimum recorded quality factor for the averaged 3 dB case was recorded at 86.7% as opposed to -25% recorded for the non-averaged case.

This averaging operation will be further illustrated in the next chapter where a simple GSM network was simulated in an attempt to gain some knowledge of the structure of the datasets that would actually be recorded by the equipment in the field.

Chapter 4

GSM Network Simulator and Display Algorithm

Introduction

A simulator is very useful tool that allows one to create datasets that closely resemble those obtained in the field. When developing a simulator, it is possible for the simulator to grow exponentially in functionality. One has identify a point after which further modelling will make insignificant difference to the "realism" of the datasets captured. The simulator was designed using a "bottom up" approach; a methodology which involves modularising the simulator into several sub modules, and then testing and integrating all of these modules into a fully functional system. Once the simulator has been constructed, we have to have some mechanism for displaying or inspecting the results. A display algorithm was developed to view the DOA estimates over time, and is discussed towards the end of the chapter.

Before beginning the simulator, careful thought had to be given to what information in the GSM standard needed to be modelled and subsequently simulated. The initial sections of this chapter present the various modules of the simulator, and are concluded with a flow diagram illustrating their inter-connectivities. A display algorithm to inspect the DOA estimates is discussed after the simulator modules and connectivities have been presented, and to conclude the chapter, two scenarios are simulated and the resulting correlation coefficients are processed and displayed.

4.1 Simulator Overview

As mentioned earlier, the simulator should be able to generate semi-realistic datasets that would closely resemble those obtained in the field. It would be preferable to have a

mechanism for configuring the simulator, where input parameters could be that specified that would "tune" the simulator output to closely match the output recorded in the field.

There are two main aspects to consider when constructing a simulator for the problem at hand. These are the GSM network itself, and the DF platform.

4.1.1 Simulator Objectives

After careful thought, the aspects of the GSM network were deemed important are:

1. The GMSK waveforms transmitted from the handsets (as these are the signals for which we wish to infer a DOA). Aspects to consider include frequency hopping, and transmitter power control.
2. The discontinuous nature of the transmission from the phone (DTX mode) as breaks in the transmission would occur, resulting in gaps in the dataset.
3. Handset mobility, as this affects the DOA algorithm output over time.
4. The number of phones in the coverage area.

A phone can potentially hand over to a new base station during a call, however a decision was taken not to model this as it would add further complexity to the simulator, which would not really contribute to developing a feel for the structure of the datasets.

Aspects of the DF platform that are considered to be important are:

1. The block sampling scheme to capture the datasets.
2. Implementation of the correlative DOA algorithm.

4.1.2 Simulator Output

The output of simulator should closely resemble the file that is written to disk by the DF platform. If the two files have identical structures, they can be processed and studied with some display algorithm. A block diagram for the simulator is shown in Figure 4.1.

This concludes an overview of the simulator. The modules for the simulator are discussed in the following section.

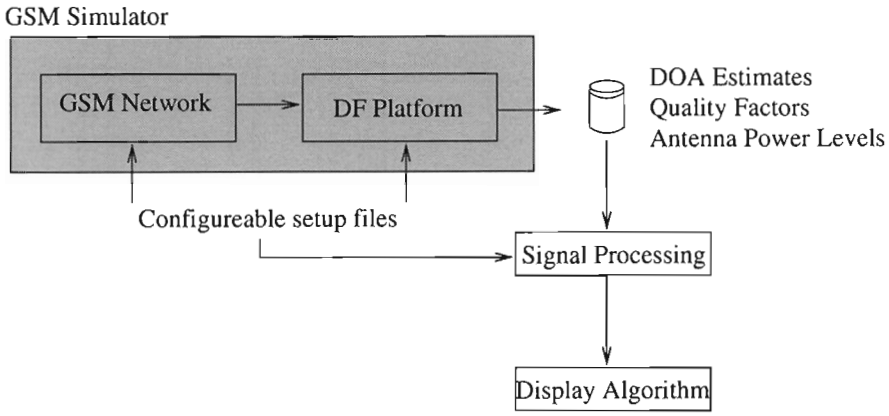


Figure 4.1: Overview of Simulator Flow Diagram

4.2 Simulator Modules

This section serves to discuss at a broad level, the various modules of the GSM simulator that were developed and integrated. The user configurable parameters for the modules have been constrained to Appendix 8.1, and should be referred to by the reader as necessary.

4.2.1 Global Co-ordinate Positioning

The first aspect to consider in the simulator is how to position the phones in some co-ordinate system relative the base station and the DF antenna. A 2D (x, y) co-ordinate system was chosen as shown in Figure 4.2.

As one can see from Figure 4.2, the five element DF antenna is placed symmetrically about the origin. The base station, and the phones may be placed anywhere in the co-ordinate space, but the phones ***must*** be positioned within a 35 km radius of the base station for the timing advance criterion to be met (c.f. Section 2.7).

4.2.2 Base Station Model

One BTS with omni-directional coverage can be placed anywhere in the scene. The BTS plays an important part in regulating both the power of the handsets, and the frequency sets over which the phones hop. Because determining the Bit Error Rate (BER) for the phones in a simulated environment would be difficult, only the minimum RXLEV value (received power level) is specified for the base station in an attempt to monitor the quality of the link between the phones and the BTS. Various parameters for the hopping algorithm are specified, together with the time slot allocation for each phone.

During the course of the simulation, the averaged RXLEV value is determined for each

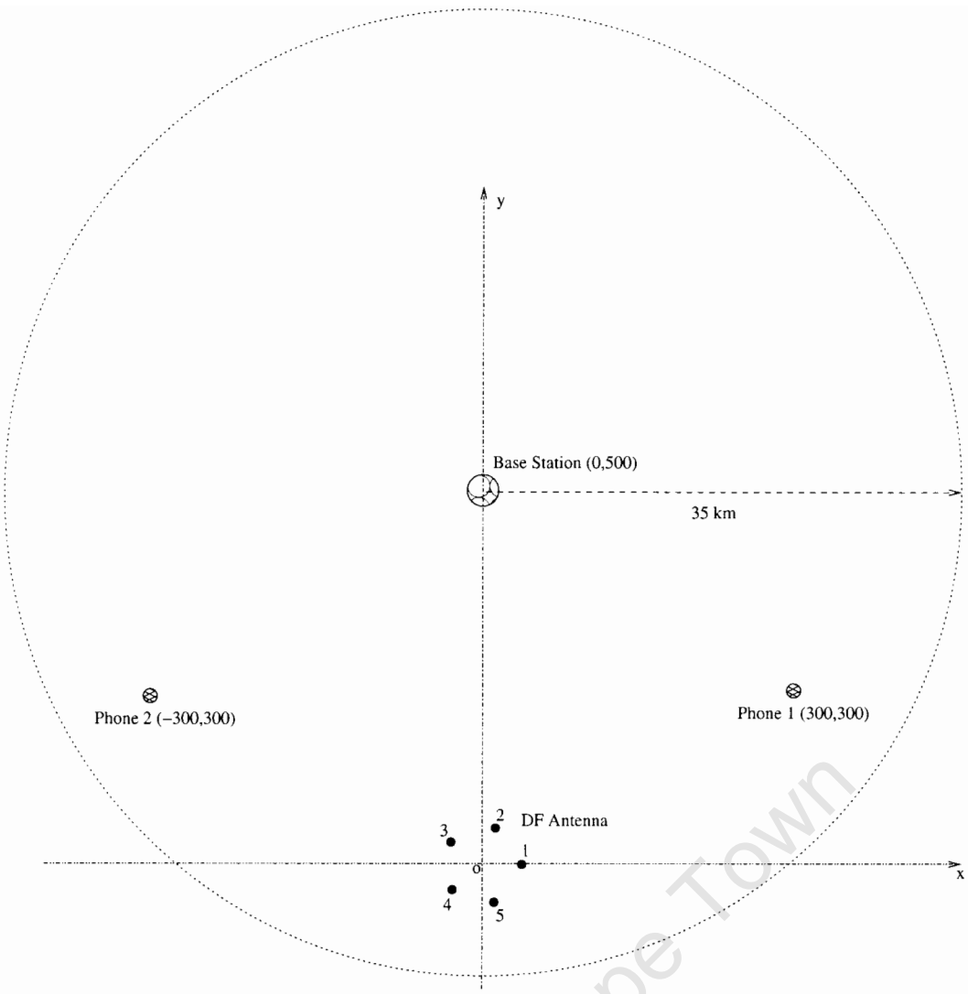


Figure 4.2: Global 2D Co-ordinate System

of the phones, and the BTS compares these with the minimum RXLEV specification and adjusts the phone power up or down by 2 dB at the end of each SACCH block (every 480 ms). The power and propagation model is discussed later in the chapter.

4.2.3 Mobile Handset Model

A mobile handset may be positioned anywhere in the scene. The phone transmits 148 bit GMSK waveforms, whose bit streams have been randomly generated. The phone as per the GSM standard, is forced to transmit on each SACCH block within the framework (every 26 TDMA frames) at a power level determined by the BTS. Transmission from a mobile as well as its position within the cell is variable during a conversation. These were modelled as follows:

Conversation Modelling

The percentage time when a subscriber actively speaks is given by the "speech activity factor," v. Measurements have shown that v takes values between 40% and 60% [10]. Consider two speakers, speaker A and B. During the time when speaker A is silent, the transmitter turns off. Background noise is sampled from speaker A, and is then played back on speaker B's side giving the illusion that speaker A is still on the line.

In order to model conversation, a random number generator was used to determine transmitter on and off times for the phones in the scene. Maximum talk time and a minimum talk time can be specified which constrains the output of random number generator to a certain range. The *same* limits are used to determine the off times for transmission.

Motion Modelling

A simple position quadratic model was chosen as the motion model. By specifying the start (x_s, y_s), intermediate (x_i, y_i), and final 2D co-ordinates (x_f, y_f) of a phone, a quadratic can be used to obtain the instantaneous (x, y) co-ordinate of a phone. The speed of motion for the mobile can be adjusted by specifying the time for the phone to move between x_s and x_f. Consider Figure 4.3.

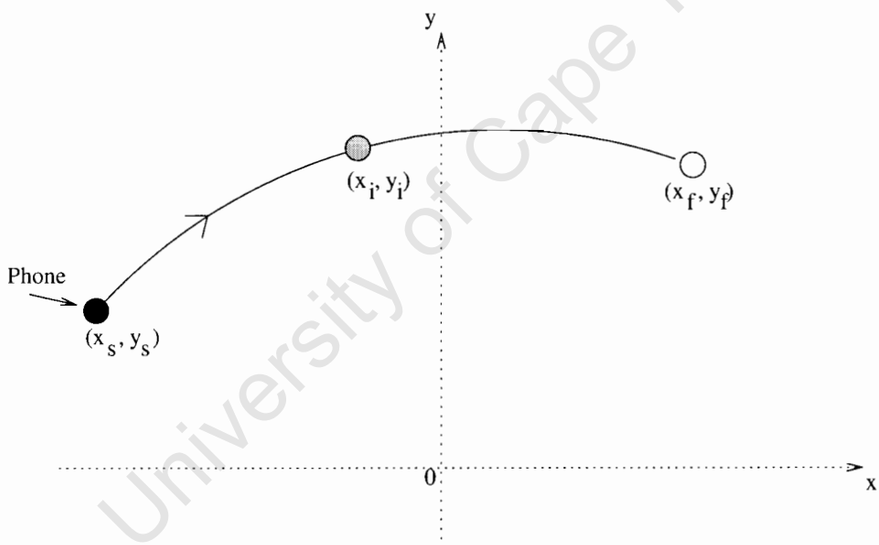


Figure 4.3: Motion Model

Let us define a quadratic: $y = ax^2 + bx + c$ where (x, y) are the instantaneous coordinates of the phone and $[a, b, c]$ are the motion model coefficients. These can be found as follows:

$$\overrightarrow{y} \quad = \quad a\ (\overrightarrow{x})^2 \quad + b\overrightarrow{x} + c \tag{4.1}$$

$$
\begin{aligned}
\begin{pmatrix} y_s \\ y_i \\ y_f \end{pmatrix} &= \begin{pmatrix} ax_s^2 + bx_s + c \\ ax_i^2 + bx_i + c \\ ax_f^2 + bx_f + c \end{pmatrix} \\
&= \begin{pmatrix} x_s^2 & x_s & 1 \\ x_i^2 & x_i & 1 \\ x_f^2 & x_f & 1 \end{pmatrix} \begin{pmatrix} a \\ b \\ c \end{pmatrix} \\
\overrightarrow{y} &= A\overrightarrow{m}
\end{aligned}
$$

From here, the motion coefficients can be calculated as follows:

$$
\overrightarrow{m} = A^{-1}\ \overrightarrow{y} \tag{4.2}
$$

Once the coefficients have been found, they are simply substituted into Equation 4.1 to calculate the instantaneous co-ordinates for the phone.

4.2.4 Block Sampling of GSM Simulated Data

Dataset Sampling

A significant portion of design time was allocated to this area of the simulator. The simulator has to be flexible enough to allow the user to vary the size of the capture blocks (80 μs by default), as well as the interval between the blocks (2 ms by default). To make the simulator efficient, it is preferable to generate the datasets as they would be recorded by the equipment on the fly, rather than generating a huge GSM dataset, and then sampling this according to the effective basebanded sample rates of the real DF equipment. The latter would produce HUGE quantities of data, and is wasteful of resources.

Mobile Time of Arrival Derivation

The time the signals arrive at the DF antenna from the phones in the radius of a cell can be computed as follows. Consider two mobile stations in a cell, namely C_1 and C_2. Let their distances from the serving base station be R_1 and R_2 and the distance from the mobile stations to the DF antenna be r_1 and r_2. This is depicted in Figure 4.4.

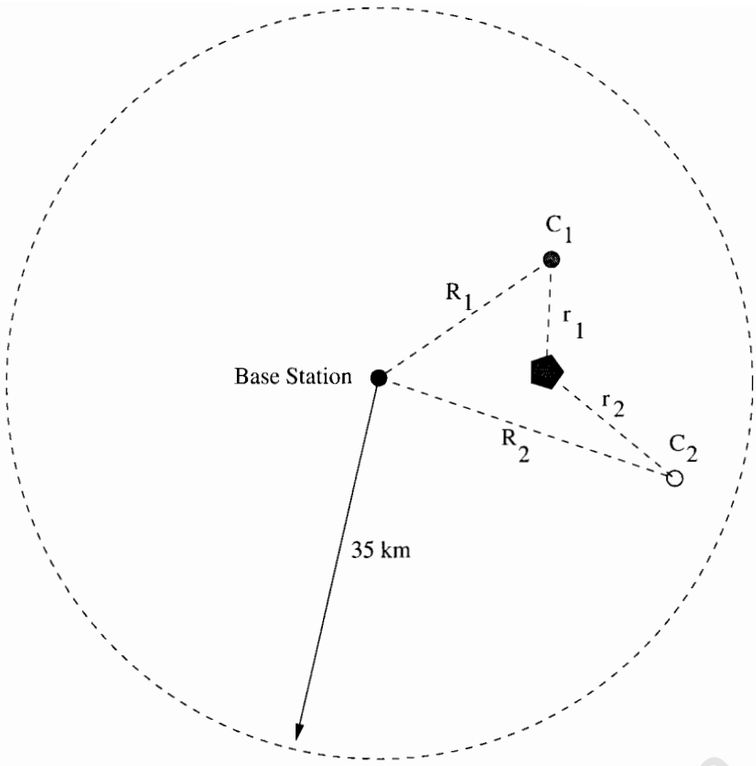


Figure 4.4: Two phones positioned in a cell

Let us now assume that the phones are in adjacent time slots (for example TS0 and TS1) and that the phones arrive at the base station in their correct time slots (i.e. the phones have already advanced their internal timing accordingly). Recall that the length of a time slot (c.f. Chapter 2.3), $T_{slot} \approx 577\,\mu s$ and comprises a burst of 148 bits, followed by a guard period of 8.25 bits. The length of a burst transmission is given by $T_{burst} \approx 546\,\mu s$.

The signal from the phones in the two time slots arrive at the base station at times t_{b1} and t_{b2} where:

$$t_{b2} = t_{b1} + T_{slot} \tag{4.3}$$

The phones transmit at times t_{c1} and t_{c2} given by:

$$t_{c1} = t_{b1} - \frac{R_1}{c} \tag{4.4}$$

$$t_{c2} = t_{b2} - \frac{R_2}{c} \tag{4.5}$$

Let us now assume that the bursts from C_1 and C_2 arrive at the DF antenna at time t_{p1} and t_{p2} given by:

$$t_{p1} = t_{c1} + \frac{r_1}{c} \tag{4.6}$$

$$t_{p2} = t_{c2} + \frac{r_2}{c} \tag{4.7}$$

By knowing when the signals from the phones arrive at the DF antenna, it is possible to compute what fraction of each signal is sampled in the $80\,\mu s$ capture window and appropriately sized blocks of GMSK data can be created.

4.2.5 Signal Propagation Model

This section presents the theory related to the propagation model that was developed into the simulator. The basebanded analytic definition of the received signal is derived, followed by the model that was used to estimate the received power level at the DF antenna. The section is concluded with a derivation for the basebanded Gaussian white noise that is added to the original signal according to the SNR at the DF antenna.

RF Signal Model

Recall from Section 2.2.3 that the GMSK waveform is given by:

$$x_{TX}(t) = Acos(\omega_o t + \phi(t) + \phi_o) \tag{4.8}$$

The analytic representation of the signal is given by:

$$x_{TX}(t) = Ae^{j(\omega_o t + \phi(t) + \phi_o)} \tag{4.9}$$

$$X_{TX}(\omega) = X_{bb}(\omega - \omega_o) \tag{4.10}$$

where $X_{bb}(\omega)$ is Fourier representation of the analytic *basebanded* signal. Let us assume a phone C_1 is some distance from the antenna. The distance from the phone to each of the elements is shown in Figure 4.5.

The propagation distance between C_1 and the ith element means that the signal $x(t)$ will arrive at each antenna element with a time delay τ_i where:

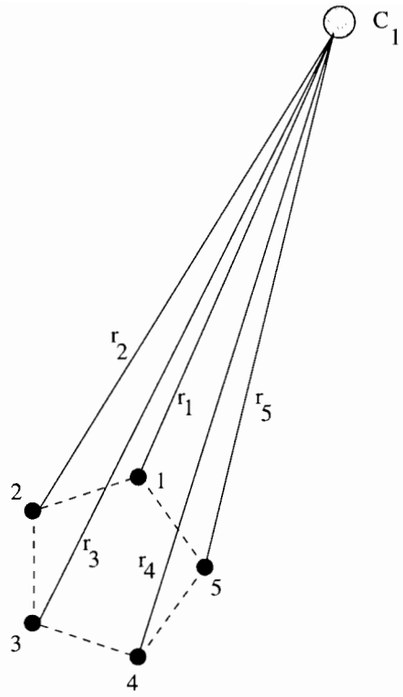


Figure 4.5: Distance of phone C_1 from 5 antenna elements

$$\tau_i = \frac{r_i}{c} \tag{4.11}$$

We will define the signal arriving at the ith antenna as:

$$x_{RX}(t)_i = \zeta_o x_{TX}(t - \tau_i) \tag{4.12}$$

$$X_{RX}(\omega)_i = \zeta_o X_{TX}(\omega) e^{-j\omega\tau_i} \tag{4.13}$$

where $X_{RX}(\omega)_i$ represents the FFT of the captured signal on the ith antenna element *before* mixing it down to baseband, and ζ_o represents an attenuation coefficient based on the propagation path between C_1 and the antenna elements.

Basebanded Signal Model

In practice, the RF signal is mixed down to an intermediate frequency, and finally to baseband where the basebanded signal is bandpass filtered and sampled by ADCs. This operation may be thought of as a translation of the entire frequency band *in view* of the antenna down to baseband.

When viewing the spectrum at RF, the carrier frequency of C_1 may not lie on the centre frequency of the DF antenna, but may be "in view" of the antenna so to speak. Let us assume that the centre frequency of C_1 is given by ω_o and that the centre frequency of the DF antenna is given by ω_{DF}. Let the spacing between them be given by $\Delta\omega$ such that :

$$\omega_{DF} = \omega_o - \Delta\omega \tag{4.14}$$

This is illustrated in Figure 4.6 (the negative frequency components have been ignored).

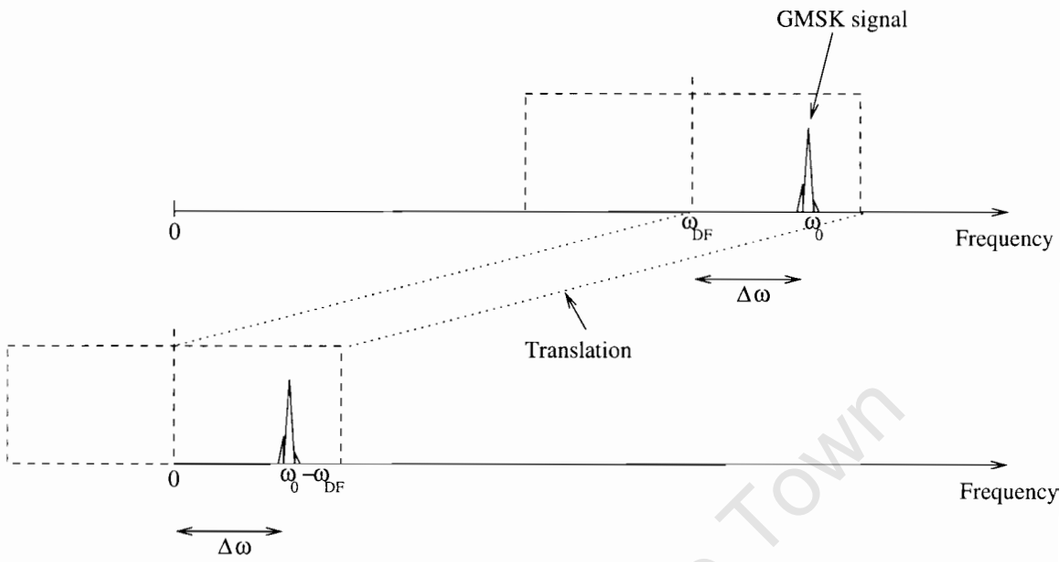


Figure 4.6: Frequency Shift Illustration

If ω_{DF} is mixed to down to baseband (DC) by an amount ω_{DF}, ω_o will be also mixed down by the same amount to a new basebanded frequency $\Delta\omega$. $X_{RX}(\omega)$ is mixed down to $X_{\Delta\omega}(\omega)$ such that:

$$\begin{aligned}
x_{\Delta\omega}(t)_i &= x_{RX}(t)_i e^{-j\omega_{DF}t} && (4.15)\\
X_{\Delta\omega}(\omega)_i &= X_{RX}(\omega+\omega_{DF})_i && (4.16)\\
&= \zeta_o X_{TX}(\omega+\omega_{DF})e^{-j(\omega+\omega_{DF})\tau_i} && (4.17)\\
&= \zeta_o X_{bb}(\omega+\omega_{DF}-\omega_o)e^{-j(\omega+\omega_{DF})\tau_i} && (4.18)\\
&= \zeta_o X_{bb}(\omega-\Delta\omega)e^{-j(\omega+\omega_{DF})\tau_i} && (4.19)\\
&= \zeta_o \left(X_{bb}(\omega-\Delta\omega)e^{-j\omega\tau_i}\right) e^{-j\omega_{DF}\tau_i} && (4.20)
\end{aligned}$$

What this means, is that if we can generate $x_{bb}(t)$ (c.f. Section 2.2.3), we can generate the basebanded analytical signal as if it were mixed down from the RF band depending on the DF antenna's centre frequency.

Received Signal Power Levels

Realistic multipath is difficult to simulate, and many variables determine the extent of the effect. There are many empirical models that exist for different environment modelling (Hata-Okumura models, and Walfisch-Ikegami models). I felt that these empirical models were too complex for the purpose of the simulator, and made use of a standard log Gaussian distribution to model the effects of short term fading proposed in Garg [20]. For outdoor environments, if the path between the DF antenna and the phone does not change regularly, the effects of long term fading are negligible.

The equation used by Garg to model the fading a distance R from the source is as follows:

$$P_{loss}(R) = 10\gamma log R + x_\sigma \tag{4.21}$$

where:

$P_{loss}(R)$	=	loss at distance R measured in dB,
γ	=	path loss exponent, (ranges between 2 in free space to 5) typically set to 4.
x_σ	=	log normal fading component, typically std. deviation of 8 dB.

Equation 4.21 was implemented and was used to calculate and adjust the power received at the base station and the DF antenna from the phones in the scene during the simulation.

Bandlimited Gaussian White Noise

Having now developed a model for the GMSK waveforms as received on each of the antenna elements (phase and frequency shifted appropriately), a derivation for the addition of bandlimited, basebanded analytic Gaussian white noise to these waveforms will be presented; such that $y(t)_i$ represents the GMSK signal as recorded on the ith antenna element. This is illustrated in Figure 4.7.

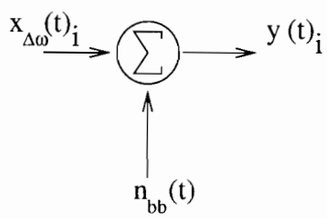


Figure 4.7: Addition of Gaussian White Noise

The Gaussian RF noise power is assumed have a flat power spectral density of $S_n(\omega) = \eta/2$. Consider Figure 4.8, which illustrates an RF band centred on f_o of bandwidth B.

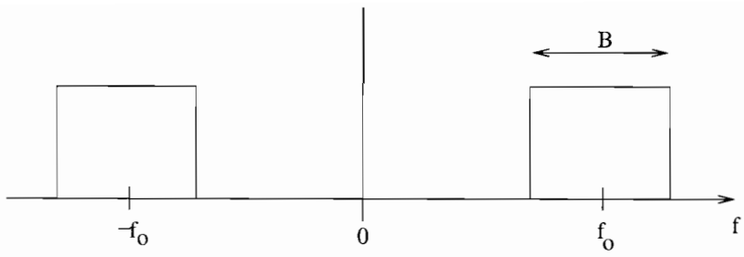


Figure 4.8: A portion of RF band, centred on f_o of bandwidth B Hz

The real noise power in this band is found to be [17]:

$$\begin{aligned} P_n &= \frac{1}{2\pi}\int_{2\pi(f_o-B/2)}^{2\pi(f_o+B/2)} S_n(\omega)\,d\omega + \frac{1}{2\pi}\int_{-2\pi(f_o+B/2)}^{-2\pi(f_o-B/2)} S_n(\omega)\,d\omega \\ &= \frac{1}{2\pi}\int_{-2\pi B/2}^{2\pi B/2} \frac{\eta}{2}\,d\omega \qquad (4.22) \\ &= \eta B \qquad (4.23) \\ &= kT_eB \qquad (4.24) \end{aligned}$$

where k is the Boltzmann's constant, T_e is the effective noise temperature where T_e= $T_{sky}+T_{receiver}$, and B is the bandwidth of the system (12.8 MHz wide by default). Stremler shows that T_{sky}, the sky noise temperature is typically of the order of approximately 300K and $T_{receiver}$, the DF antenna noise temperature is approximately 100K. This makes the effective noise temperature equal to approximately 400K.

Recall that the real GMSK waveform is given by:

$$x_{RF}(t) = Acos(\omega_o t + \phi(t) + \phi_o)$$

Rather than trying to compute the amount of noise for a given signal power, it would be easier to assume a basebanded signal power of 1W, i.e. $\overline{x_{\Delta\omega}(t)_i^2} = 1W$, and to scale the amount of noise that is added to the signal according to the SNR at baseband. The RF signal to noise ratio is a ratio of the signal power to the noise power at RF, and is given by:

$$\begin{aligned} SNR_{RF} &= \frac{\overline{x_{RF}(t)^2}}{P_n} \\ &= \frac{\frac{1}{2}A^2}{kT_eB} \qquad (4.25) \end{aligned}$$

The complex analytic basebanded noise power, is given by:

$$\sigma_{bb}^2 = E\left\{|n_{bb}(t)|^2\right\} \tag{4.26}$$

where $n_{bb}(t)$ is the complex stationary Gaussian noise signal. For the RF SNR to remain constant when the signal is mixed down to baseband, the following must be true:

$$\begin{aligned} \frac{\overline{x_{RF}(t)^2}}{kT_eB} &= \frac{\overline{x_{\Delta\omega}(t)_i^2}}{\sigma_{bb}^2} \\ \sigma_{bb}^2 &= \frac{kT_eB}{\overline{x_{RF}(t)^2}} \end{aligned} \tag{4.27}$$

Because $n_{bb}(t)$ is complex, at any instant it has associated with it some real component I and some imaginary component Q such that:

$$n_{bb} = I + jQ \tag{4.28}$$

Equation 4.26 may be extended as follows:

$$\begin{aligned} \sigma_{bb}^2 &= E\left\{n_{bb}(t)^2\right\} \\ &= E\left\{I^2 + Q^2\right\} \\ &= E\left\{I^2\right\} + E\left\{Q^2\right\} \\ &= \sigma_I^2 + \sigma_Q^2 \end{aligned} \tag{4.29}$$

Because the standard deviation of the noise in the real and imaginary parts is equal, $\sigma_I^2 = \sigma_Q^2$ it follows that, $\sigma_{bb}^2 = 2\sigma_I^2$. Substituting this into Equation 4.27, we see that the power for the I and the Q channels is:

$$\sigma_I^2 = \frac{kT_eB}{2\overline{x_{RF}(t)^2}} \tag{4.30}$$

$\overline{x_{RF}(t)^2}$ can be computed using Equation 4.21. If the transmission power, P_{TX} and the

distance from the transmitter to the DF antenna, R are known, $\overline{x_{RF}(t)^2}$ is given by:

$$\overline{x_{RF}(t)^2} = P_{Tx} - P(R) \quad (dB) \tag{4.31}$$

The dB value can then be converted to a normal gain, and substituted back into Equation 4.30.

Dataset Processing

After bandlimited white noise has been added to each of the antenna datasets, processing is performed before the sets are written to disk. This involves applying a Blackman Window to the datasets, to suppress sidelobes introduced by the bandlimiting action of the receiver, and truncating the datasets to produce a dataset with a bandwidth specified by the user. For example, with the current sample rate of 12.8 MHz and a capture window of $80\,\mu s$, a 1024 point FFT is produced. If the user selects a 10 MHz bandwidth, the 1024 point FFT is reduced to 800 points by discarding the edge of the frequency band which results in an FFT bandwidth of 10 MHz.

Once the datasets have been windowed and truncated, the correlation coefficients are calculated (c.f. Section 3.4) and an estimated direction of arrival is computed for each bin. One this has been done, these estimates, together with the associated quality factor and the averaged power spectrum (dBm) are written to disk.

4.3 Simulator Flow Diagram

Having described the main modules, their inter-connectivities are summarised in a high level flow diagram depicted in Figure 4.9. To begin with, the phone positions in the scene must be updated to reflect the new positions as a result of the motion path model. We must then determine which phones are active in the TDMA frame (some may be inactive due to DTX mode), and of these phones, what portion of the transmitted information is sampled by the DF platform. After this has been determined, GMSK waveforms are generated for the phones which have been sampled. The length of these waveforms is determined by what fraction of the waveform has been captured by the DF platform. After the basebanded datasets have been generated, appropriate phase shifts in the frequency domain are applied, and Gaussian white noise is added to the dataset before applying a smoothing window.

When the datasets have been prepared, the aperture products are formed and are passed to the DOA algorithm. From here the DOA estimates for each frequency bin are computed and written to disk, together with the associated quality factors and the averaged levels

on the antennas[1]. Once the direction estimates have been written to disk, a check is made as to whether an entire SACCH frame has passed. If it has, the mobile power is updated depending on the averaged signal strength measured at the base station during the SACCH frame.

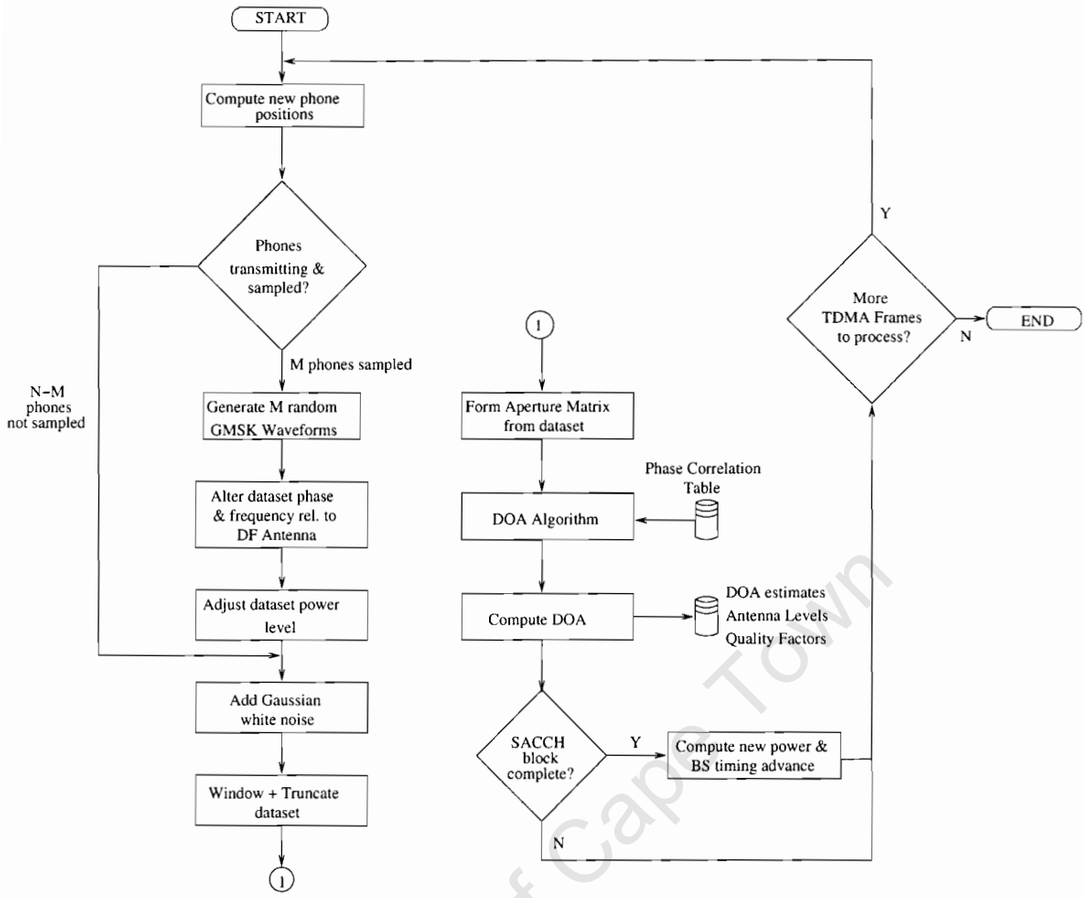


Figure 4.9: Simulator Flow Diagram

This concludes a discussion of the simulator that was developed. The display algorithm is presented next.

4.4 Display Algorithm

Recall that the DF platform samples $80\ \mu s$ of data every 2 ms, and that a time slot repeats every 4.6 ms. As a result of this sampling mismatch, a particular time slot moves in and out of view of the capture window over time. This is more clearly shown in Figure 4.10 where TS0 can be seen moving in and out of the $80\ \mu s$ capture window.

[1]Note that later in the chapter, we will see the advantage of averaging the aperture information about the GSM carriers, before writing the DOA estimates to disk.

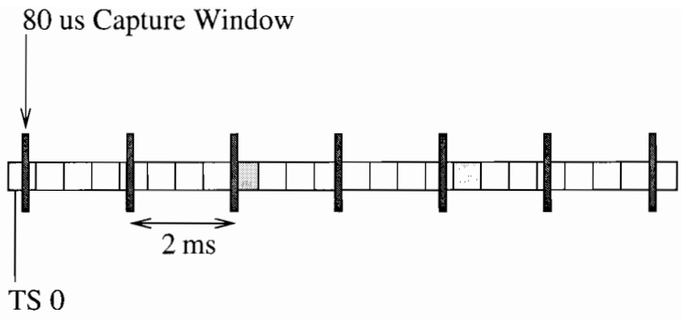


Figure 4.10: DF Platform Sampling of Timeslots

This moving in and out results in short gaps between in the dataset. Because the transmitter of the phone may also be turned off during a period when the time slot is in view of the capture window (DTX mode) , the interval between sample instants where the timeslot is hit is not constant and large gaps may appear in the dataset (this is observed later).

For small datasets (of the order of one second of recorded GSM data), the results for each capture can be displayed one after the other. However, for large datasets (of the order of several minutes), it would be impossible to display all the data points sequentially in one window, due to the size of the files written to disk. As a result, we can either display every nth capture, or try to compress the data somehow for displaying. We will call these methods of display, *Display Option 1 and 2* respectively, and will discuss them shortly. Recall from the previous section that after each capture, a DOA estimate for each frequency bin, the corresponding quality factor for this DOA estimate, and the averaged power levels for the five antenna elements are written to disk. We will define a *captured frame* as being the data obtained from one capture.

Two plots can be generated from the data recorded, a spectogram, and a estimated DOA plot. Depending on the chosen display option, each vertical line in time for the spectogram represents the averaged power spectrum for each of the five antenna elements. The DOA plot indicates the directions of arrival for content in that frame. The spectogram data is thresholded above the noise floor to focus solely on the mobile transmissions. By extracting the frequency components above a particular power threshold, and then extracting from these, components above a certain quality factor threshold (say 85%), it is possible to map the frequency axis to a DOA axis.

4.4.1 Display Option 1

Display Option 1 was the first display option explored, and entails displaying the data periodically i.e. displaying every nth captured frame. Each line of the spectogram represents the data in that frame that exceeds the thresholds set on both the amplitude levels, and quality factors. The danger in displaying every nth frame is that due to the irregular mo-

bile transmission times, not all captured frames would contain good DOA estimates. As a result, some frames containing potentially good DOA estimates could be skipped over. The severity of this increases as the dataset becomes larger, as more captured frames must be skipped over to display the entire file. This will be highlighted in an example after the discussion of Display Option 2.

4.4.2 Display Option 2

In order to display ALL the data in one plot, *Display Option 2* entails grouping portions of captured frames together and compacting them into a single *display frame*. The number of captured frames that are grouped together into one display frame is determined by the number of frames there are in the dataset for a given number of physical pixels over which the data can be displayed. This would be advantageous over Display Option 1 as *all* the data in the dataset is considered.

Because several frames of captured data are grouped into one display frame, successful *detections* (DOA bins for which the levels in the corresponding frequency data exceed the imposed amplitude and quality factor thresholds), should be grouped together in such a way that if one detection occurs for a particular frequency bin and several detections occur for adjacent frequency bins, the two display frames would appear as "bright" as each other in the final display frame. This ensures that detections have equal weighting for each display frame, irrespective of how many detections occurred in the corresponding captured frames. Essentially, this is an OR operation of the successful detections and is performed for each DOA bin along the captured frames that constitute one display frame. This is can be more clearly understood by referring to Figure 4.11, where the grey squares indicate successful detections within the *captured* frames, and the black squares represent whether a detection has occurred or not in a particular *display* frame. Let us assume we are trying to compress two captured frames, into one display frame.

As we can see from Figure 4.11, the display frame either contains a detection or is blank with no intermediate colour levels due to the ORing operation. The 8 captured frames have been condensed into 4 display frames.

Having discussed the two display options, we will now evaluate the effectiveness of both when applied to two simulated datasets.

4.5 Simulation Scenarios

This section presents the results of scenarios that were modelled to acquire datasets that resemble those acquired by the real DF platform. Two scenarios are presented involving a number of phones moving in predetermined paths.

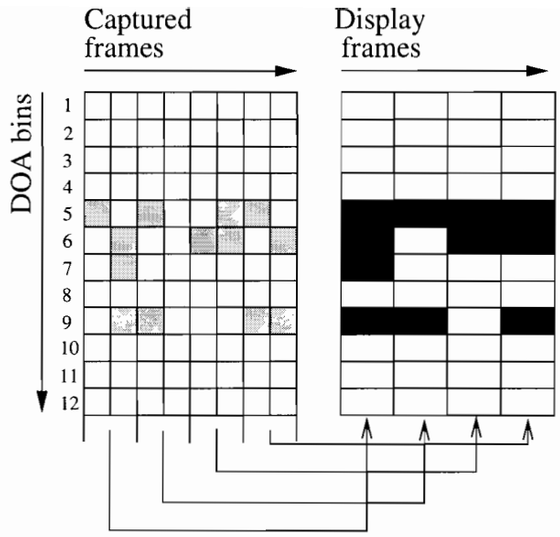


Figure 4.11: The transformation of captured frames into display frames

4.5.1 Scenario 1

Geometry

To test the simulator, GSM data were simulated for approximately 138s (30000 TDMA frames). Three phones (power class 4) were simulated in time slots 3, 3 and 4. The base station was arbitrarily allocated ARFNs = [13, 20, 33, 48] which correspond to frequencies [892.6, 894, 896.6, 899.6] MHz. The geometry for the scenario is illustrated in Figure 4.12. The MAIO for which to seed the slow frequency hopping was set to [0,1,2], and frequency hopping was activated. This means that the three phones at the start of the simulation were allocated frequencies 892.6, 894, and 896.6 MHz.

During the course of the simulation, phone 1 and phone 3 move along the lines indicated so that the output of the DOA can be verified. We should observe that phone 1 moves from $DOA = 45°$ to a $DOA = 90°$, phone 2 should remain stationary, and phone 3 should move from a $DOA = 270°$ to a $DOA = 0°$.

Results

The results of the simulation of Scenario 1 are shown in Figure 4.13 (spectogram plot), and Figure 4.14 (DOA plot) for Display Option 1. Figure 4.15, and Figure 4.16 illustrate the spectogram and DOA plots for Display Option 2. Recall that Display Option 1 displays every nth frame of data. The dataset length as mentioned earlier is 138s (30 000 TDMA frames). This length translates into $\frac{138s}{2ms} = 69000$ captured frames. Let us assume we wish to display the information in 1024 display frames. This means that $\frac{69000}{1024} = 67$ captured frames must be skipped in order to fit the entire dataset into the 1024 display

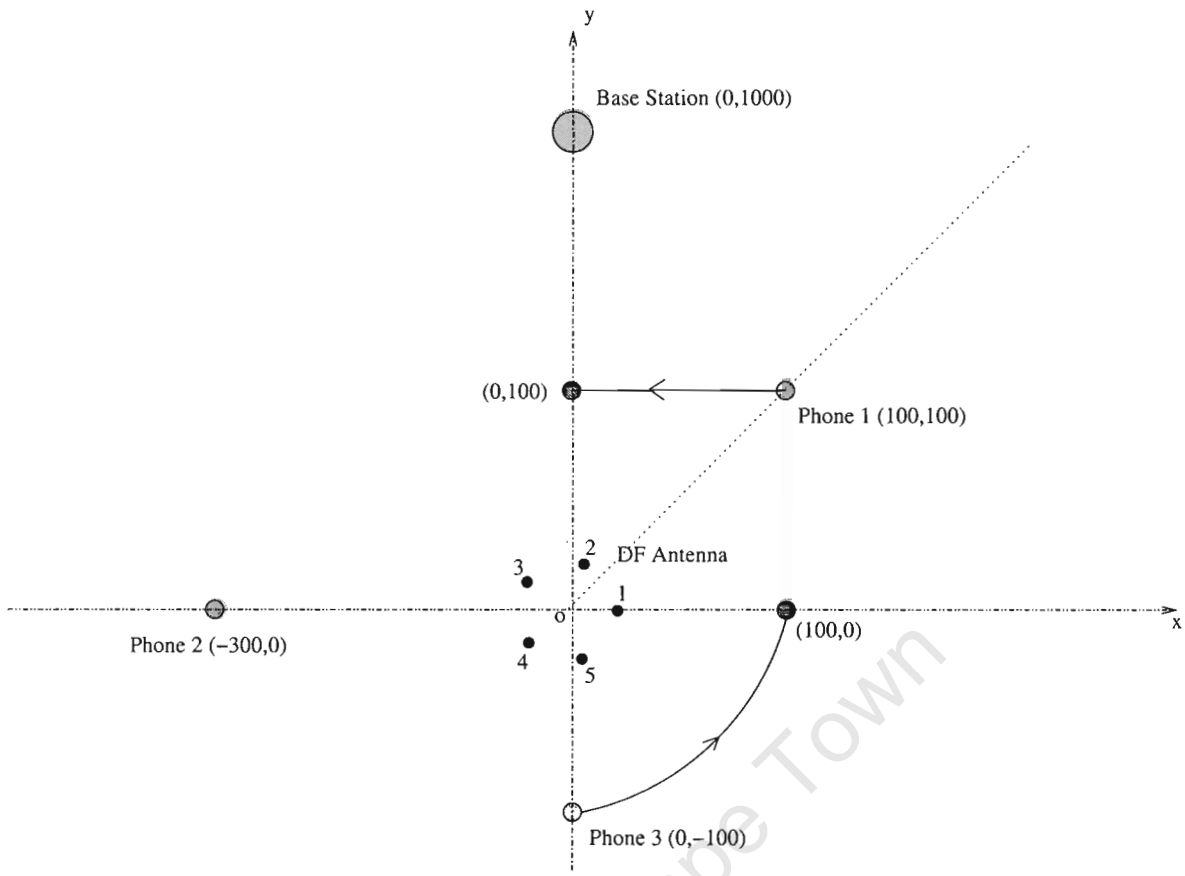


Figure 4.12: Geometry for Scenario 1

frames.

If we inspect Figure 4.13, we can see a series of streaks on each of the carriers. These are captured GMSK waveforms emitted from the phones over time. The spacing between the streaks is not constant as predicted in Section 4.4. The larger gaps are periods where the phone is turned off i.e. no speech is present. The shorter gaps occur as a result of the capture window moving in and out of the time slot during periods where the transmitter is activated (c.f. Figure 4.10). Observe that some of the streaks in the plot are broader than others. This is because some of the captured GMSK waveforms are truncated prematurely (the amount of premature signal truncation is dependant on how the time slot aligns with the capture window at the time of sampling), resulting in a broadening of the main lobe.

Visually, without a-priori knowledge, it is difficult to see from the spectogram plot how many phones were actually present in the area, and whether or not they were hopping across the four carriers. To try and predict the number of phones from the spectogram plot, a more detailed inspection of the time slot information would have to be made.

The corresponding DOA plot for Display Option 1 can be seen in Figure 4.14. The amplitude threshold was set at -30 dBm, and the quality factor was set at 95%.

From this plot, we can clearly distinguish between the three phones. Phone 1 can be seen moving from $DOA = 45°$ down to $DOA = 90°$. Phone 2 remains stationary on

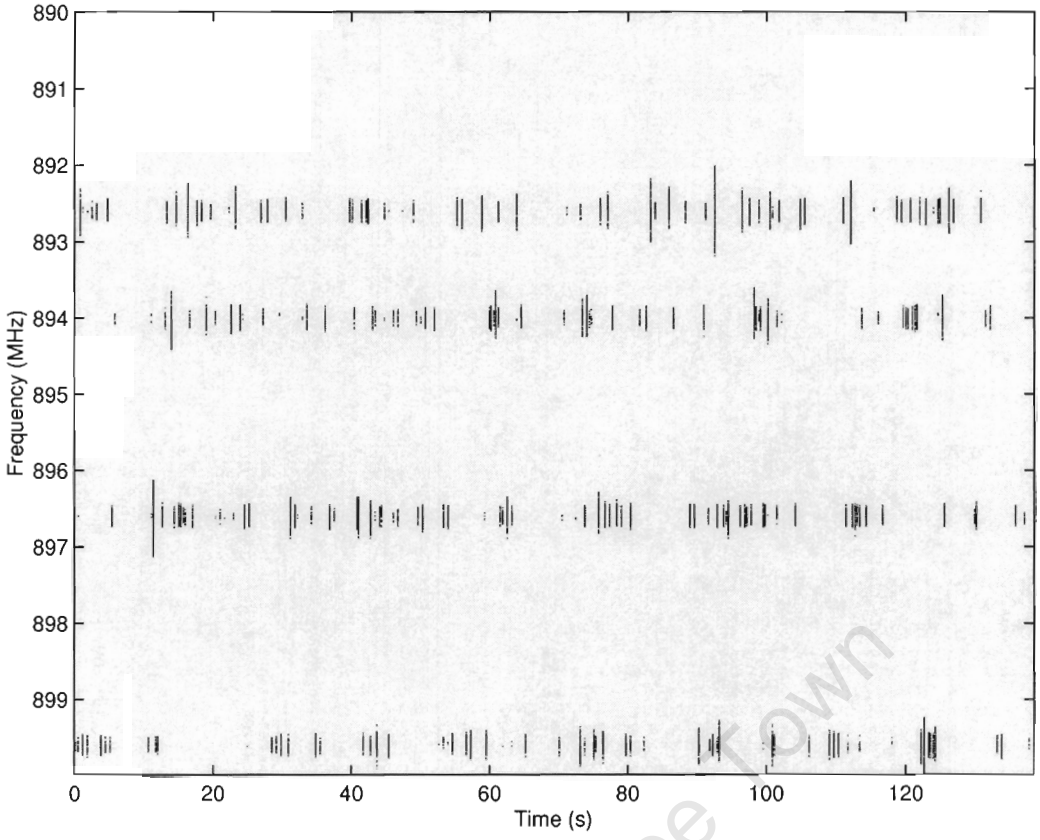


Figure 4.13: Spectogram for Scenario 1 - Display Option 1

$DOA = 180°$ and phone 3 can be seen moving from $DOA = 270°$ to $DOA = 0°$. The gaps in the dataset are consistent with those from the spectogram dataset are due to the same reasons the gaps appear in the spectogram.

Having observed the datasets displayed with Display Option 1, we will now observe the entire dataset as viewed with Display Option 2. By maintaining the number of display frames at 1024, rather than skipping every 67th capture frame, 67 captured frames are condensed into one display frame. This yields a spectogram shown in Figure 4.15. We can see immediately, that more information is displayed in Figure 4.15 when compared with Figure 4.13. For example, if we look at each carrier for the first 20s of data, significantly more data is observed for Display Option 2.

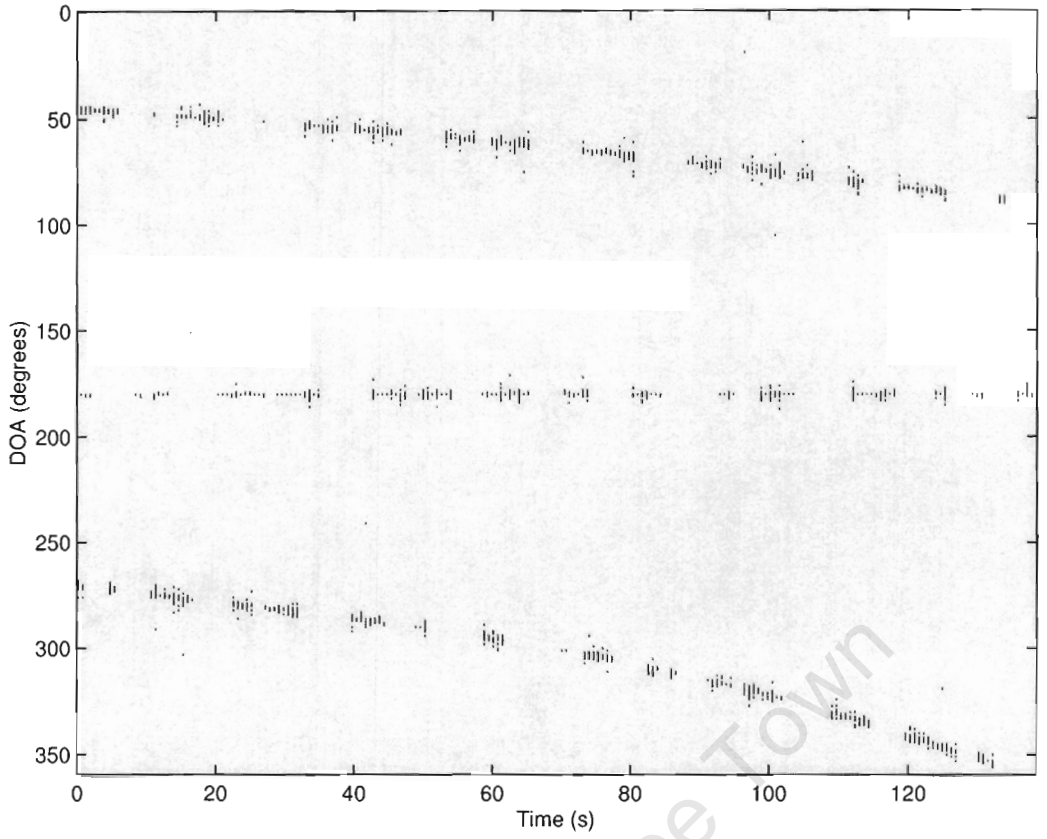


Figure 4.14: DOA for Scenario 1 - Display Option 1

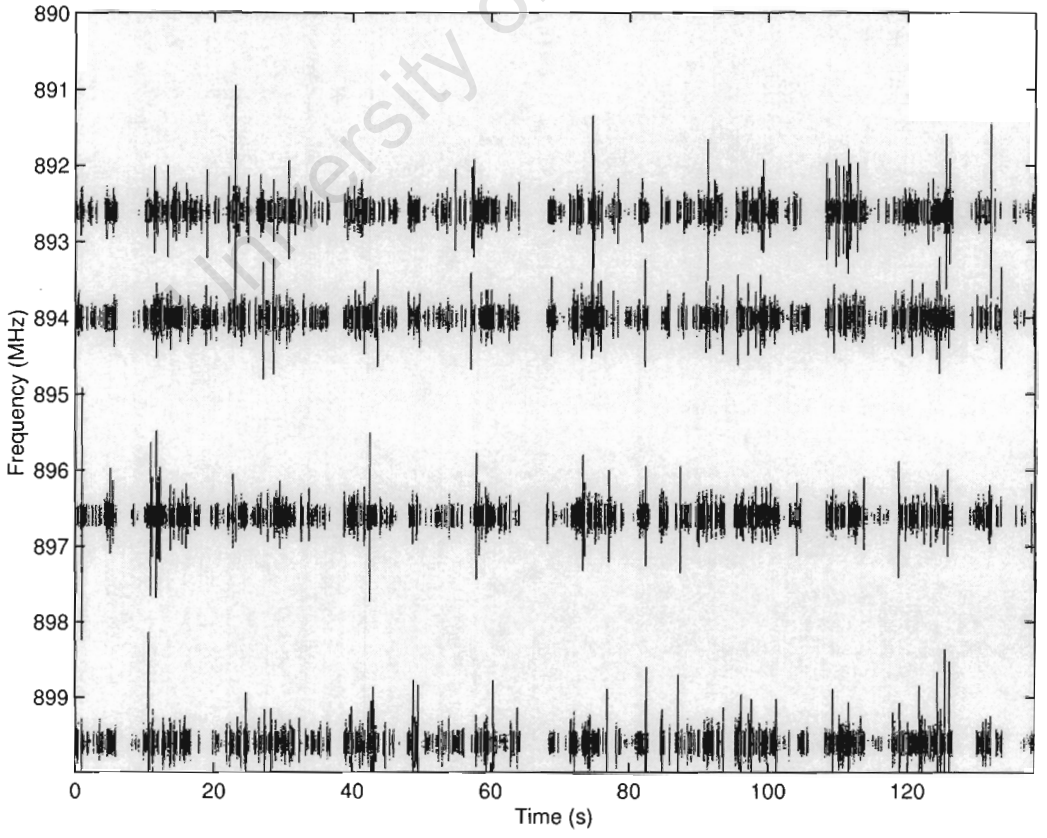


Figure 4.15: Spectogram for Scenario 1 - Display Option 2

The corresponding DOA plot is shown in Figure 4.16. Note that the level and quality factor thresholds were maintained.

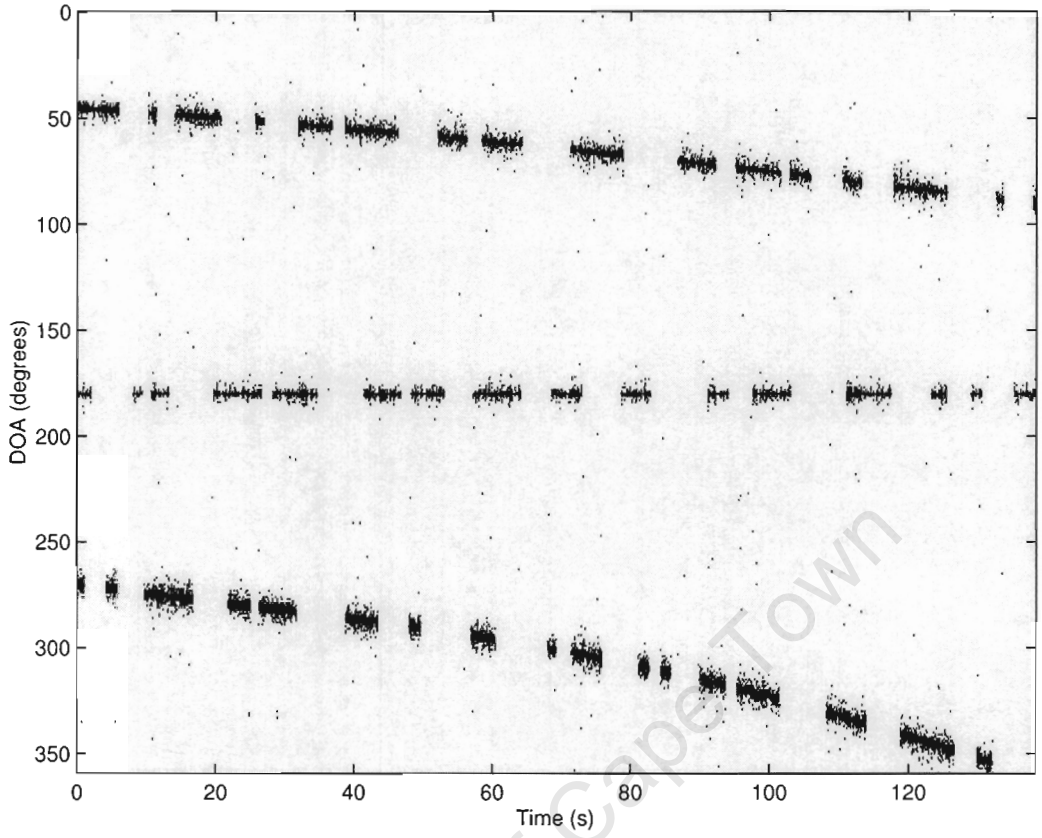


Figure 4.16: DOA for Scenario 1 - Display Option 2

If we compare Figure 4.16 with Figure 4.14, we note that estimated DOAs are significantly more dense during periods where transmissions occur. This is to be expected, as every datum in the dataset is considered. By visually comparing the two plots, we can see that Display Option 2 provides one with a greater certainty of the paths the phones are traversing over time.

One disadvantage of Display Option 2, is that the fusing of the captured frames into one display frame results in the loss of the timing information for each captured frame. By maintaining the timing information (as was done for Display Option 1), an algorithm could potentially be written to try and determine which data points belong to which timeslots in an attempt to track the phones individually. This is beyond the scope of the thesis, and is addressed in the conclusions. As we wish to focus on visual tracking, focus will be moved more towards the refinement of Display Option 2. As Display Option 2 considers *all* of the captured frames (including frames containing poor DOA estimations), Display Option 2 can possibly be improved further and is discussed after Scenario 2 has been presented.

4.5.2 Scenario 2

Geometry

From the DOA plot in the first scenario (using Display Option 2), it was easy identify three phones in the area. However, what if there are two phones in the area, and they cross each other? Keeping the simulation parameters the same for this scenario, let us remove phone 3, and position phone 2 as depicted in Figure 4.17.

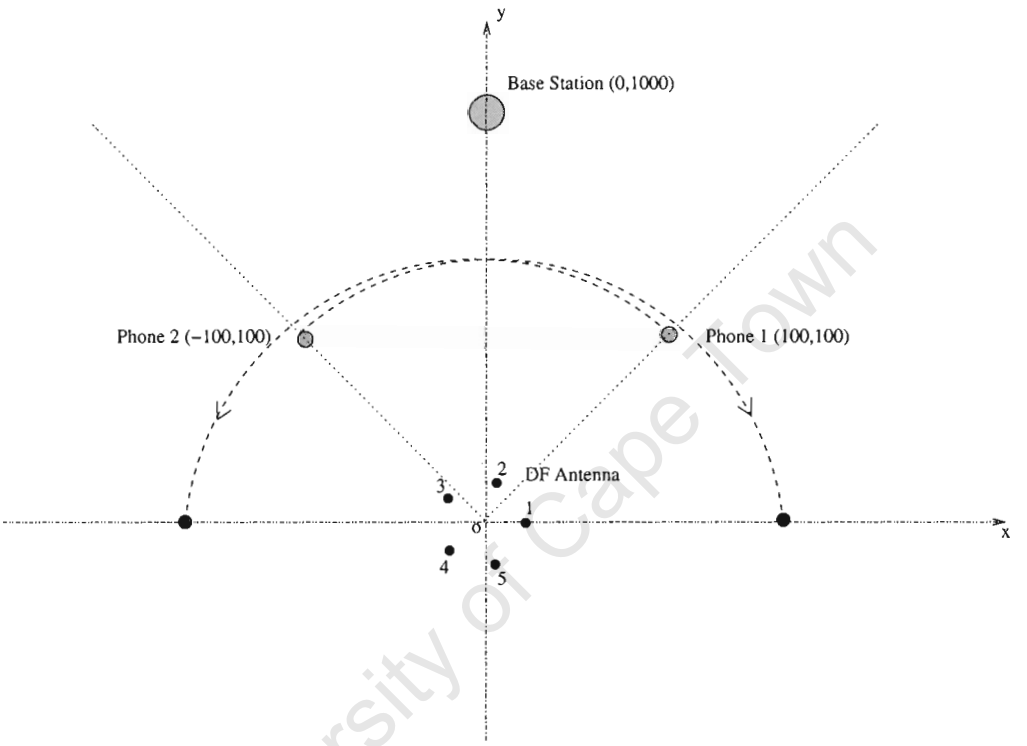


Figure 4.17: Geometry for Scenario 2

Results

The results for the simulation output are shown below in Figures 4.18 and Figure 4.19 using Display Option 2. The level and quality factor thresholds were maintained from the previous scenario.

The spectogram in Figure 4.17 looks similar to that in Figure 4.15, which suggests again that it would be difficult to determine the number of phones from the spectogram plot (at first glance).

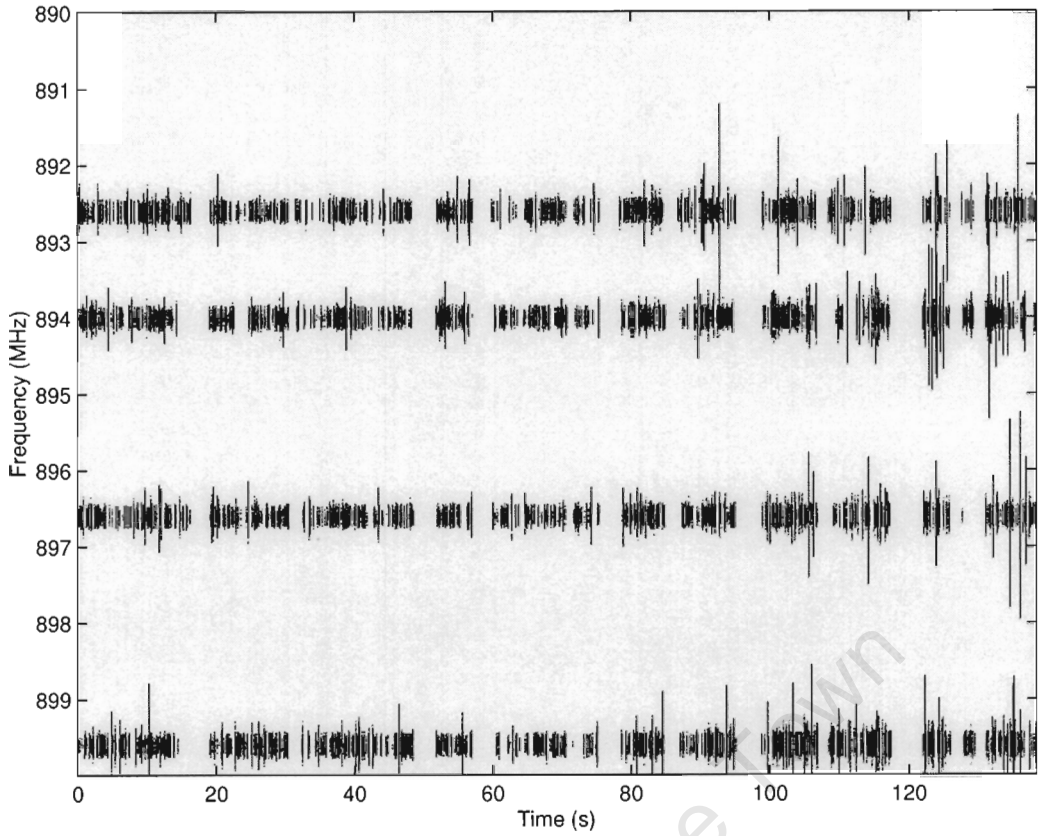


Figure 4.18: Spectogram for Scenario 2

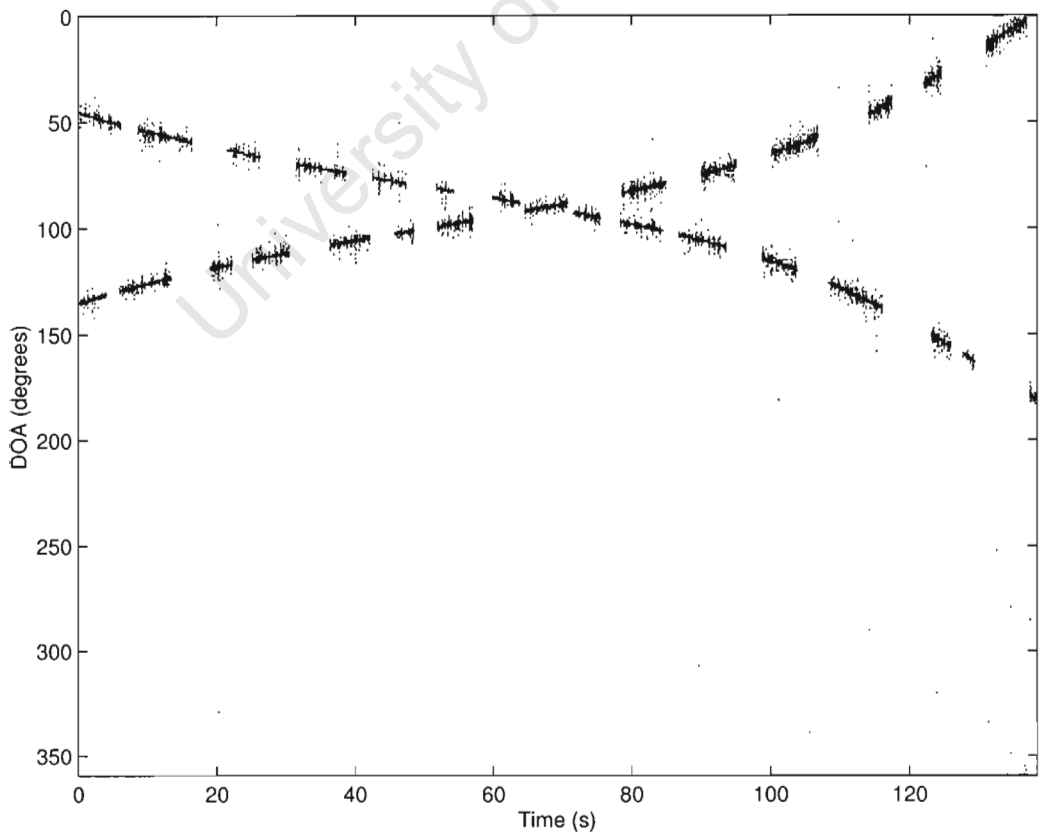


Figure 4.19: DOA for Scenario 2

Inspection of the DOA plot, reveals that the phones cross at approximately $t = 65s$. However, if we had not known the motion path of the phones a-priori, we would not have known from this plot whether they had crossed, or separated from each other at the crossing point which makes visual tracking difficult.

If we look carefully at the DOA image, we can see that occasionally, speckles occur at arbitrary directions of arrival. This is because the level threshold is not sufficiently high to discard these points (by making it too high, some useful data points may be also be discarded). What we do notice from the DOA plots from both scenarios (implementing Display Option 2), is that these erroneous speckles do not occur in clusters, which means that if we extend the display model to include a 2 dimensional convolution smoothing kernel, and then threshold the data after the application of the kernel, these isolated speckles can potentially be eradicated. Points occurring in clusters will be amplified by the convolution operation, and will cause them exceed the threshold that is applied after the convolution of the kernel with the dataset.

4.5.3 Extension of Display Option 2

Rather than performing an OR operation of the detections along the captured frames constituting one display frame for each DOA bin, each detection in a captured frame (the grey blocks in Figure 4.11) is assigned a value of 1, and these detections are summed over the captured frames constituting one display frame. This results in varying levels per display bin, as opposed to a simple 1 or 0 from display frame to frame as was the case for Display Option 2.

This can more clearly be understood by inspecting Figure 4.20 which shows how the display frames differ from those in Figure 4.11. Let us assume that we are trying to compress 4 captured frames into one display frame.

As we can see, the display frame bins have varying levels depending on how many detections occurred in the captured frames. If a Gaussian smoothing kernel is now convolved with the display frames and then thresholded appropriately, the pixelated image in Figure 4.16 and Figure 4.19 can be converted to those depicted in Figure 4.21 and Figure 4.22. The degree to which the pixels are smoothed in the plot is controlled by the size of the kernel, and the roll off in both the time and DOA axes.

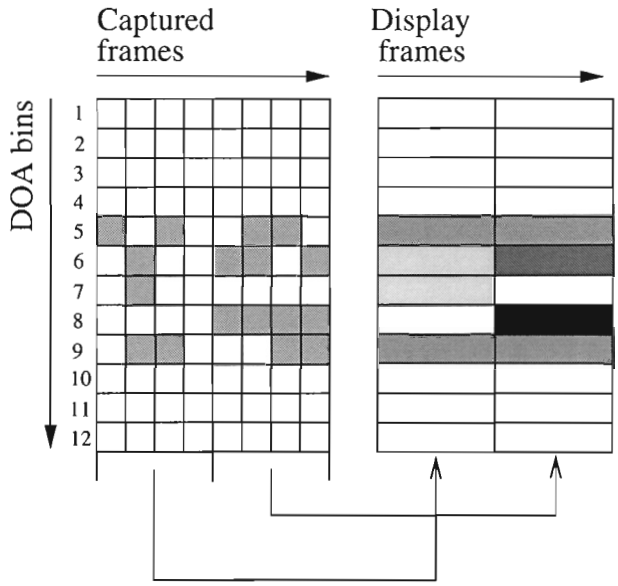


Figure 4.20: Compressing the DOA estimates from 8 captured frames into 2 display frames

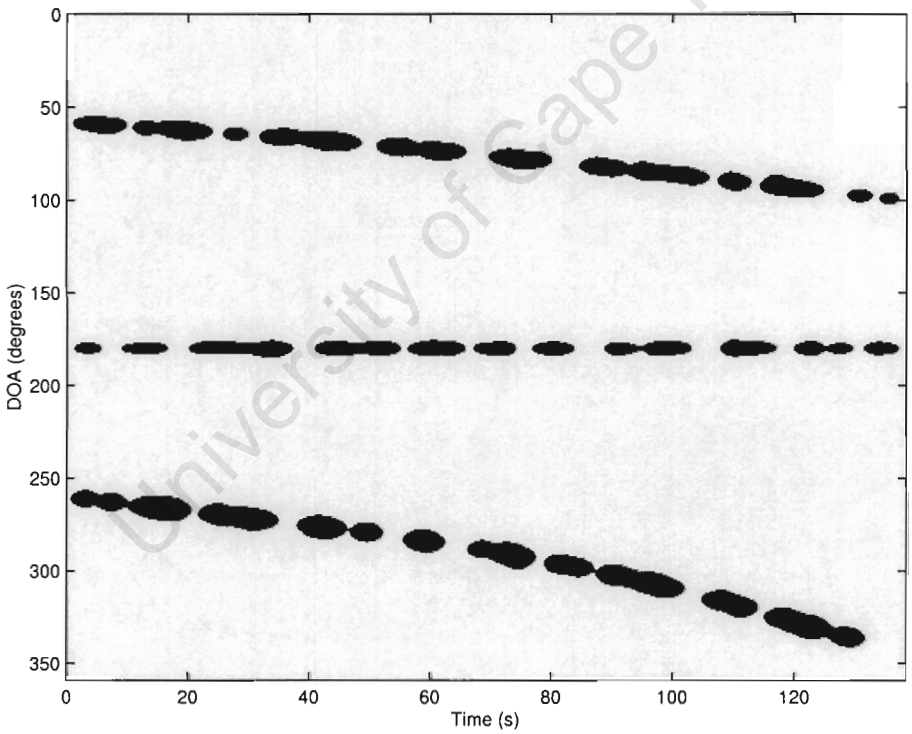


Figure 4.21: Improvement of DOA Estimate Plot from Scenario 1

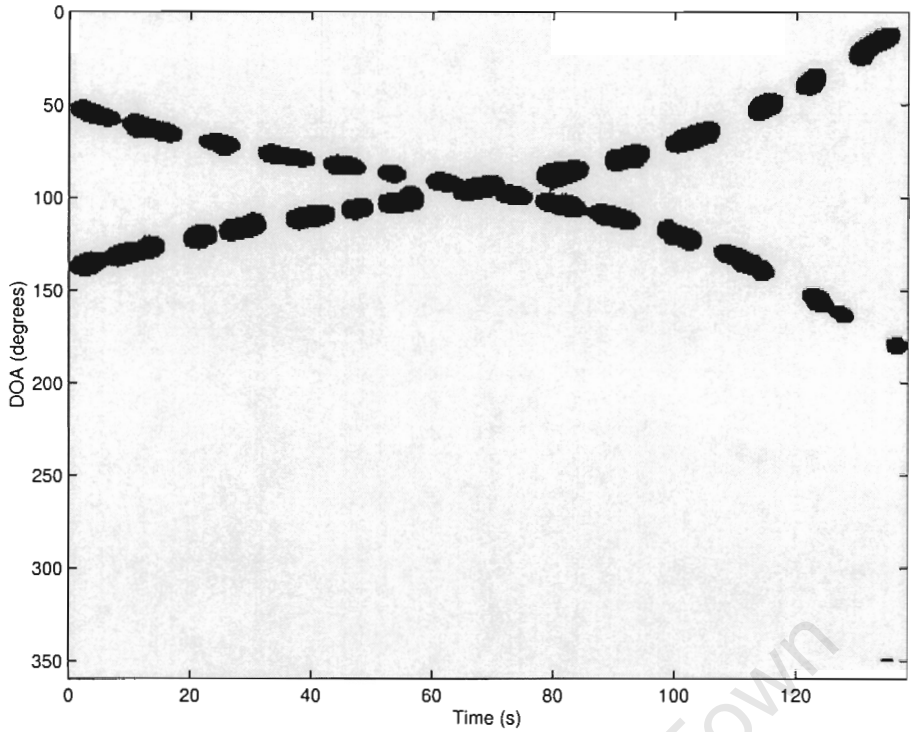
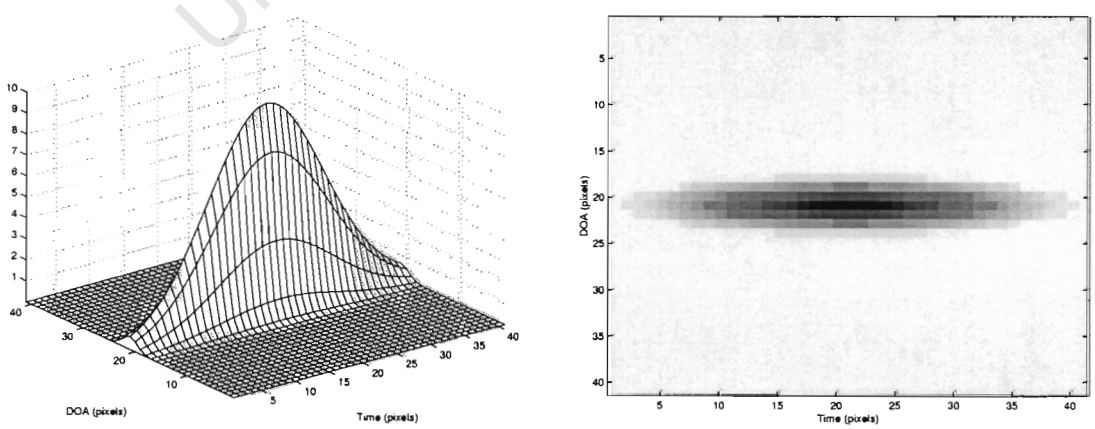


Figure 4.22: Improvement of DOA Estimate Plot from Scenario 2

We can see from Figure 4.21 and Figure 4.22, that the pixels in close proximity with each other have been fused together. The thresholding operation has removed a significant portion of the isolated pixels from the plot, and we can see that because of the shape of the kernel (depicted in Figure 4.23), more smoothing has occurred over the time axis in an attempt to connect adjacent regions. Notice that the kernel roll off in the DOA axis is significantly less, as we want to try to maintain direction resolution.



(a) 3D Representation of Kernel

(b) Top view of Kernel

Figure 4.23: Gaussian Smoothing Kernel

4.5.4 Incorporating GSM Carrier Information to Improve DOA Estimation

We have seen so far that condensing all the information in the dataset into several display frames, is better than displaying every nth frame of data. The smoothing kernel to try and group adjacent DOA estimates did so at the expense of degraded angular resolution. Recall in Section 3.8, that a possible improvement that one might make to the DF algorithm, would be to average the aperture information over the bins where the GSM carriers reside. This should reduce the speckles seen around the true DOA in Figures 4.16, and 4.19.

In order to observe this change to the DOA plots, the aperture information was first averaged around the GSM carriers before passing the resulting new aperture information to the DOA algorithm, where the computed estimates were written to disk as before. Using Display Option 2, and the same level and quality thresholds for each of the Scenarios, the following DOA estimation plot was observed for Scenario 1 in Figure 4.24 and Scenario 2 in Figure 4.25.

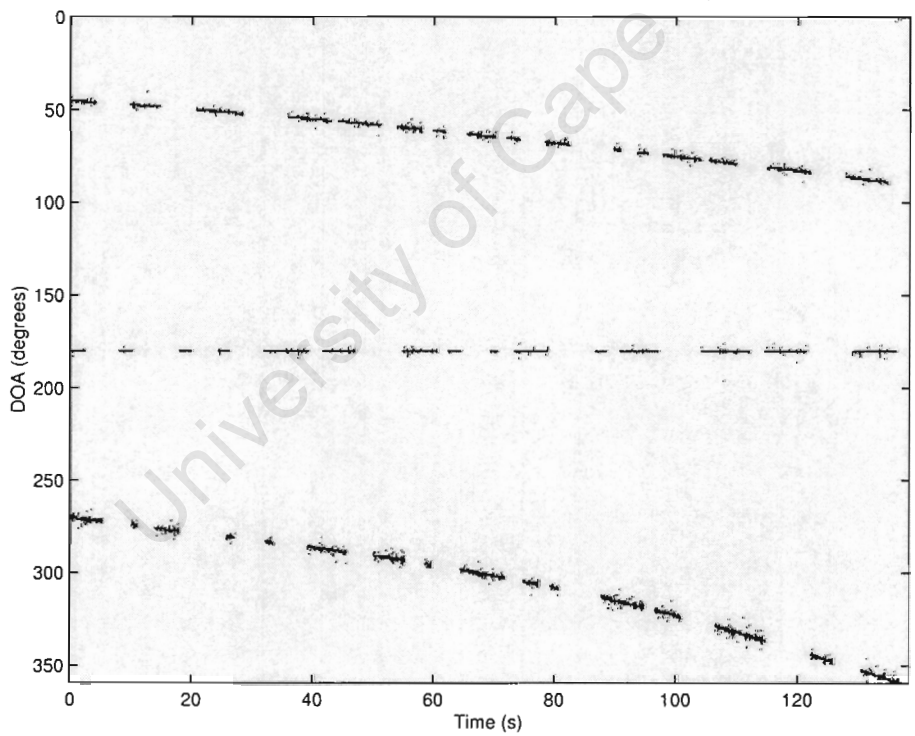


Figure 4.24: DOA Estimate Improvement for Scenario 1

We can see from the averaging operation, that the erroneous DOA estimations (speckles) have been reduced significantly. The speckled points around the true DOA for the phones have also been reduced, and most have converged on the true DOA which suggests that this method would be the best way to process and display the data.

There are several scenarios that can be potentially be explored. Because this DOA technique is sensitive to several wavefronts at the same frequency impinging on the antenna

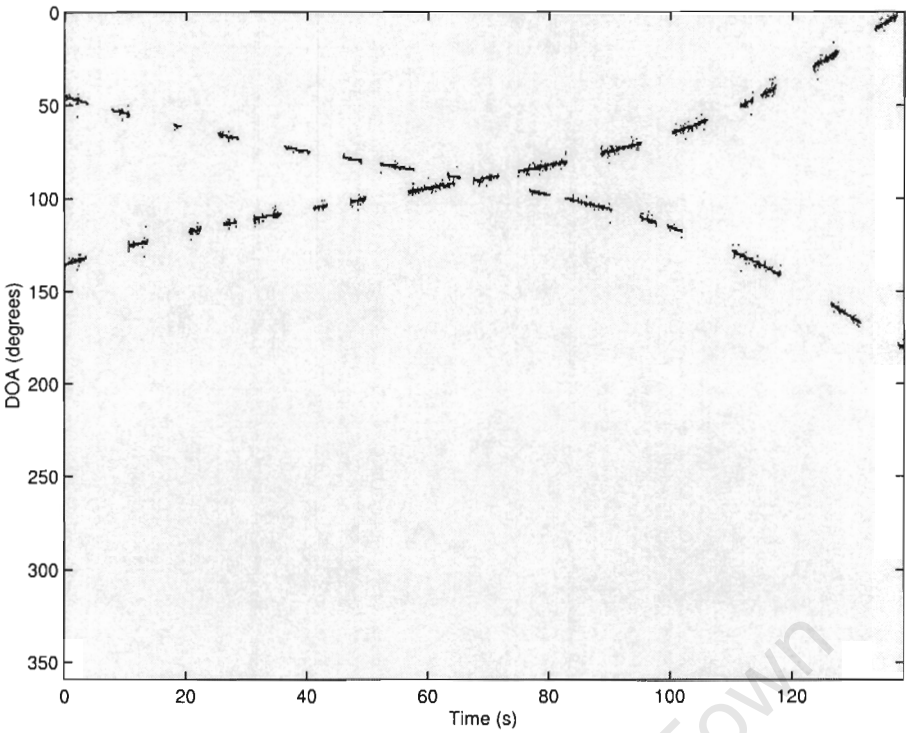


Figure 4.25: DOA Estimate Improvement for Scenario 2

at the time of sampling, an investigation was conducted to assess if this situation could potentially occur in a GSM coverage area. The results of the investigation are presented in the next chapter.

Chapter 5

Time Slot Sampling Investigation

5.1 Introduction

We have seen that it is possible for the block sampling strategy employed by the current DF system (described in the Section 3.3) to detect mobile phones in an area, and to provide a estimate of the DOA for each burst captured from a particular phone. From the simulations discussed in the previous chapter, gaps in the data were seen due to a particular time slot fading in and out of view (c.f. Section 4.4). The severity of the fading is related to the ability of the DF hardware to sample an active time slot from TDMA frame to frame. How often is a time slot viewed by the 80 μs capture window? This chapter addresses this question, and statistics are provided accordingly for simulations conducted.

If all the mobiles in the coverage of a single BTS are allocated the same frequency by the BTS, then all the phones must have unique timeslots for a burst collision at the BTS to be avoided. In cases where phones have been allocated adjacent timeslots, the internal timing mechanism of the phone must be advanced to compensate for the range delay (c.f. Section 2.7). Due to the variations in timing advances for the phones in an area, a situation may arise in which the signals can actually overlap at the DF antenna, depending on its position relative to the BTS and the phones in the area of coverage. This situation is also addressed in the chapter, and statistics related to a scenario where the worst case occurence of an overlap at the DF antenna are provided.

5.2 Time Slot Sampling

Recall that a mobile once allocated a time slot, maintains this time slot for the duration of the call even if frequency hopping takes place. We have seen in previous chapters, that due to the block sampling nature of the DF platform, a particular time slot fades in and out of view during a conversation. If there was some periodicity to this fading in and out,

it would be possible to "follow" a timeslot during the duration of a call if the sampling location relative to the TDMA frame is known at the start of sampling.

To compute the periodicity of the alignment of the start of the capture window with the start of the TDMA frame period, we essentially need to compute the lowest common multiple (LCM) of the TDMA frame period with that of the interval between capture blocks. Recall that the length of a TDMA frame is defined to be exactly 60/13 ms. Let us also assume that the sampling instant is in *exact* multiples of 2 ms. If sampling commences with the start of the capture block aligned with the start of TS0, exact realignment will occur after 13 TDMA frames have passed. This is because:

$$\begin{aligned} 1\,TDMA\,frame &\longleftrightarrow \frac{60}{13}\,ms \\ 13\,TDMA\,frames &\longleftrightarrow 60\,ms \end{aligned}$$

With a spacing between capture blocks of 2 ms, the sampling pattern repeats after 30 capture blocks.

Simulations were conducted to develop more of a feel for how often a particular time slot is "hit" (in view of the capture window) given the fact that the spacing between captured blocks is 2 ms.

Before providing the results of the simulations, consider Figure 5.1 which clarifies the situation.

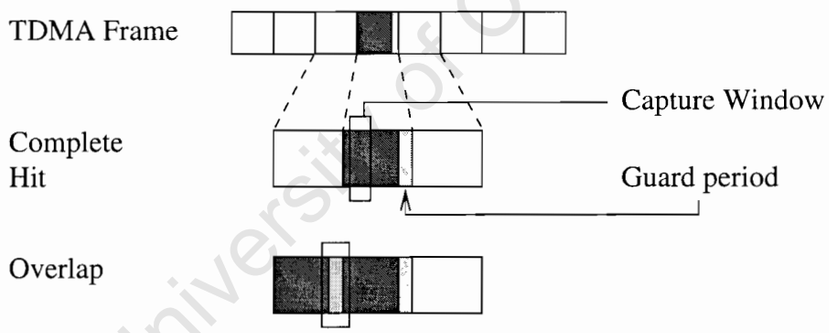


Figure 5.1: Time Slot Capture Definitions

The grey block indicates the time slot of interest in the TDMA frame. A "complete hit" occurs if the capture window is completely sampling the transmission of a time slot or if the capture window is in the guard period of an adjacent time slot and overlapping into the time slot under investigation (since there is insignificant transmission during the guard period). An "overlap" is said to occur if the capture window captures portions of transmissions from two adjacent time slots.

5.2.1 Results

Eight phones were simulated in each of the eight timeslots. Over the course of 13 TDMA frames, observations of complete hits and overlaps were recorded. The simulation parameters are as follows:

Simulation Parameter	Value
Capture window length	80 μs
Period between samples	2 ms
Simulation length	0.06 s
No. TDMA Frames	13
No. samples recorded	30

Table 5.1: Time Slot Sampling Simulation Parameters

We wish to know what percentage of the time slots that can potentially be sampled, are actually sampled as either complete hits or overlap hits. Ideally we would want complete hits for all of the time slots to avoid ambiguities. However with a continuous block sampling scheme such as the one that is currently implemented, we shall see that this isn't possible unless the timing of the period between the blocks is altered in some fashion.

The simulation was started with the start of the capture block aligning to the start of TS0 (time slot 0). The results for the simulation are shown below:

Parameter	TS0	TS1	TS2	TS3	TS4	TS5	TS6	TS7
% Complete Hits	30.77	23.08	23.08	23.08	30.77	23.08	23.08	23.08

Figure 5.2: Results recorded given 13 TDMA frames available for sampling

Overlaps were observed to occur between TS7 and TS8 in Frame 1, and then between TS6 and TS7 in Frame 2. A similar overlap pattern occurred between TS3 and TS4 in Frame 8 and between TS2 and TS3 in Frame 9. These erroneous overlaps account for 13.3% of the total samples recorded for the duration of the 13 TDMA frames.

Turning our attention to TS0, a plot of how often the time slot is hit completely over the 13 TDMA frames is given in Figure 5.3.

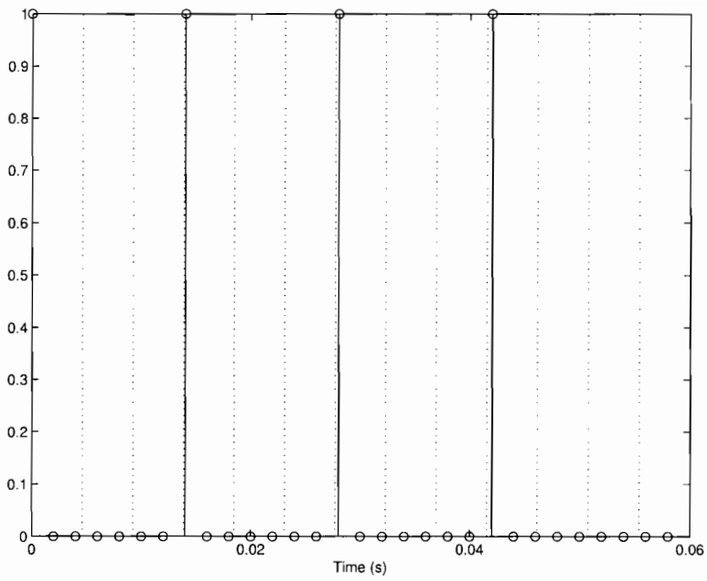


Figure 5.3: Plot illustrating the complete hits of TS0

The solid vertical bars in the plot indicate the times when TS0 is in view of the capture window. The dotted lines indicate the start of a new TDMA frame (also the start of TS0). The round circles on the time axis indicate a miss of TS0. It would appear that if synchronisation is achieved, we can expect to hit the same time slot, after 7 samples.

What should be noted at this point is that if perfect synchronisation does **not** occur at the start of sampling, the results shown above would be significantly different (we may observe more overlaps, and less complete hits depending on where the capture window is positioned inside the TDMA frame). What we do know though is that the pattern of the results would still repeat every 13 TDMA frames due to the modular nature of the TDMA access scheme.

5.3 Time Slot Overlap Investigation

Until now, a study has been conducted which basically assumes that the signals arriving at the DF antenna all arrive in sequence without any collision. For a GSM cell, this observation would only be possible if the DF antenna was at the base station. If the DF antenna is somewhere else in the cell, the signals arriving at the DF antenna would not necessarily be in a predictable sequence as the propagation delays between the phones and the DF antenna would be different. Depending on where the phones are positioned in the cell, significant overlap of the signals could occur at the DF antenna. To add to this, depending on where the sampling begins within the TDMA frame, differing results would be observed over the duration of the 13 TDMA frames.

This derivation for the times of arrival of the signals emitted from two mobile stations in a cell, namely C_1 and C_2 was covered in Section 4.2.4. Recall that their distances from the serving base station were R_1 and R_2 and that the distance from the mobile stations to the DF antenna were r_1 and r_2. A copy of the Figure 5.4 has been included for easy reference:

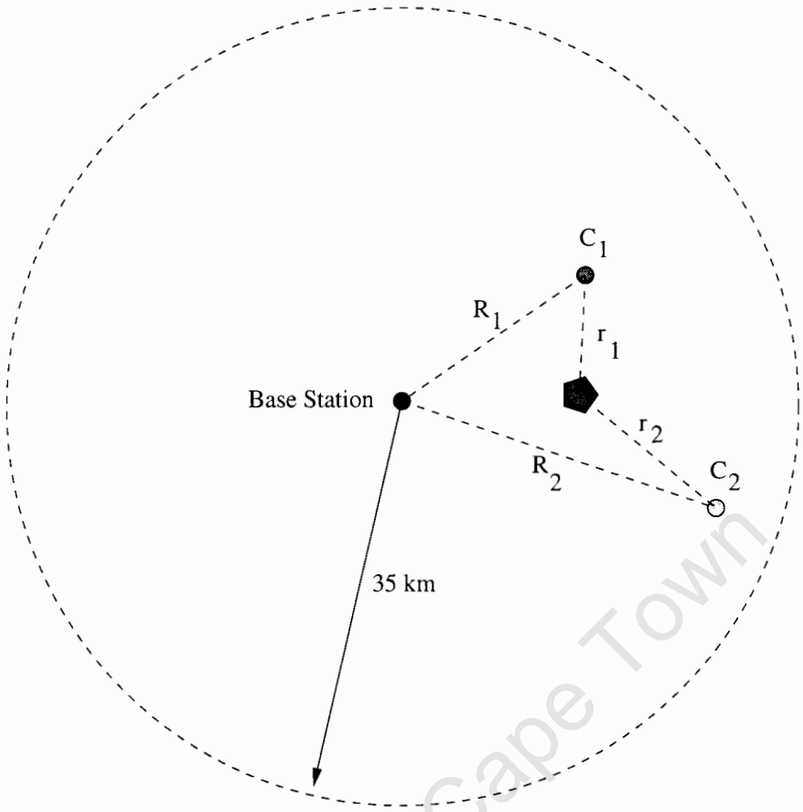


Figure 5.4: Two phones positioned in a cell

The bursts from C_1 and C_2 arrive at the DF antenna at time t_{p1} and t_{p2} given by:

$$t_{p1} = t_{c1} + \frac{r_1}{c} \tag{5.1}$$

$$t_{p2} = t_{c2} + \frac{r_2}{c} \tag{5.2}$$

where t_{c1} and t_{c2} are the times of transmission at the start of the burst. Assuming that there is a negligible amount of power in the guard period at the end of the time slot (there may be a small amount due to the the roll off of the frequency filter), a burst overlap is said to occur at the DF antenna if:

$$t_{p2} < (t_{p1} + T_{burst}) \tag{5.3}$$

where T_{burst} is the duration of the 148 bit GMSK transmission (547 μs). Given Equation 5.3, the amount of overlap, T_o, is given by:

$$\begin{aligned} T_0 &= (t_{p1} + T_{burst}) - t_{p2} \\ &= (t_{c1} + \frac{r_1}{c} + T_{burst}) - (t_{c2} + \frac{r_2}{c}) \end{aligned} \tag{5.4}$$

A timing diagram depicting the occurence of an overlap is given in Figure 5.5.

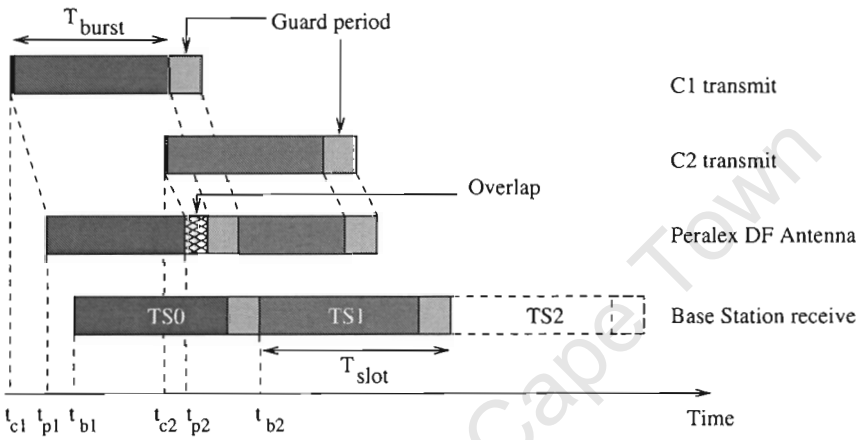


Figure 5.5: Timing diagram for two phones in a cell

The task we are now faced with, is deciding where in the cell the phones should be positioned in order for maximum overlap to occur at the DF antenna.

As we have also observed in Section 5.2, it is possible for both bursts to exist within the capture window without physically overlapping at the DF antenna for an erroneous result to occur (for example the end of a burst from C_1 and the start of a burst from C_2). While the signals from the two phones are not overlapping in time, an FFT is performed on the datasets, which combines the two signals in the frequency domain. If the phones are making use of the same carrier, this produces erroneous DOA estimates for that capture. As the burst overlap increases, the potential for more erroneous recordings also increases.

5.3.1 Geometry Investigation for Worst Case Overlap

As mentioned earlier, we would like to know where the two phones should be placed, such they produce a maximum physical overlap at the DF antenna (i.e. maximising Equation 5.4). If we inspect Equation 5.4, we see that this amounts to maximising t_{p1} and minimising t_{p2} subject to the constraint identified in Equation 5.3.

Placement of the first phone C_1

We wish to maximise t_{p1} for maximum overlap to occur. Substituting Equation 4.4 into Equation 5.1, results in:

$$t_{p1} = t_{b1} + \frac{1}{c}(r_1 - R_1) \tag{5.5}$$

As t_{b1} and t_{b2} are both constants separated by T_{slot}, we can make $t_{b1} = 0$ and $t_{b2} = T_{slot}$. The maximum value r_1 can attain is if the phone C_1 is as far away from the DF antenna as possible. This occurs when the DF antenna is on the edge of the cell, and the phone is at the opposite end of the cell. Consider Figure 5.6.

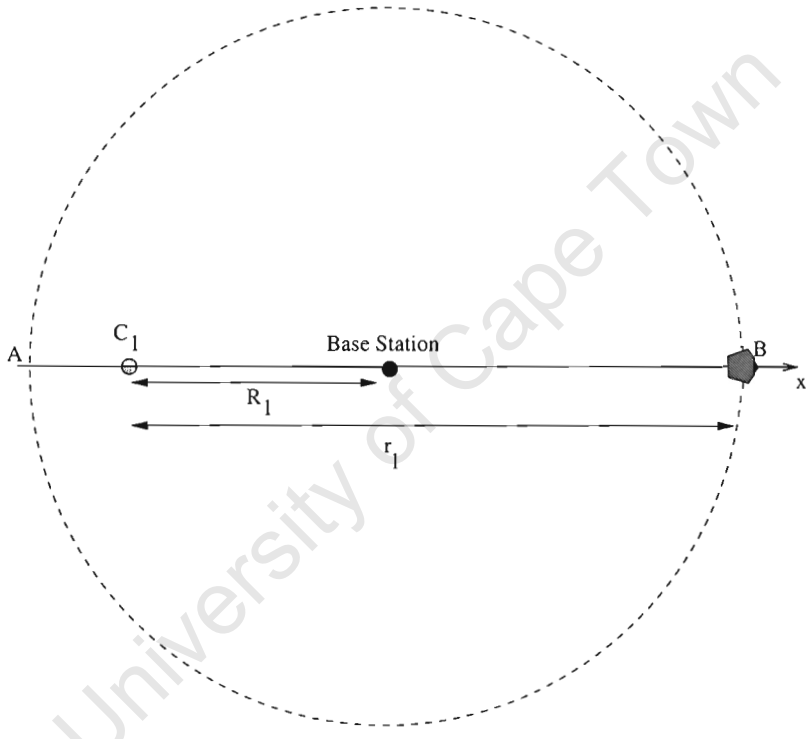


Figure 5.6: Moving a phone from A to B

Because the phone has to advance its timing mechanism the further away it moves from the base station, it turns out that if we inspect how $r_1 - R_1$ varies as the phone is moved along the x axis from A to B, we observe the following in Figure 5.7.

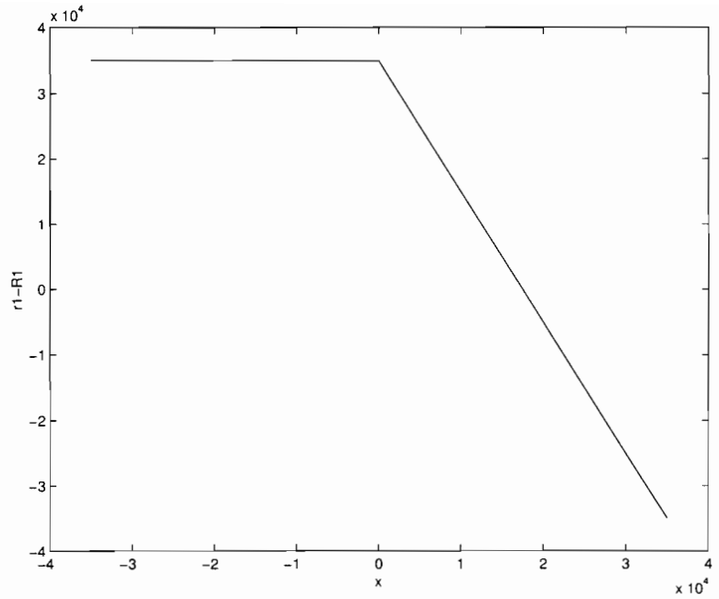


Figure 5.7: Variation of the distance between C_1 and the base station relative to the DF antenna

This means that if the phone exists anywhere in a line between the point A and the base station, the time of arrival at the DF antenna is constant.

Placement of the second phone C_2

If we substitute Equation 4.5 into Equation 5.2, we are left with:

$$t_{p2} = T_{slot} + \frac{1}{c}(r_2 - R_2) \tag{5.6}$$

Inspection of Equation 5.6 suggests that t_{p2} is a minimum when $r_2 = 0$ i.e. (when the phone is on top of the DF antenna) and when the phone is on the border of the cell. Using the information derived in Section 5.3.1, we see that the worst case overlap occurs when the phones are positioned as shown in Figure 5.8. Note that C_1 may be anywhere along the line between A and the base station.

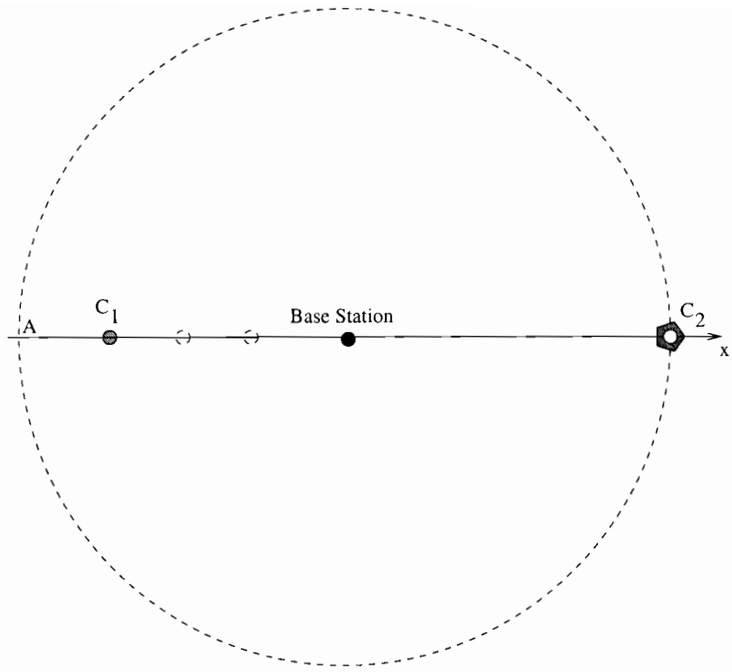


Figure 5.8: Phone placement for worst case time overlap

5.3.2 Worst Case Overlap Results

If the phones are positioned as shown in Figure 5.8, the maximum amount of overlap was found to be (using equations proposed in Section 5.3):

$$T_0 = 203\,\mu s \tag{5.7}$$

This amount of overlap is two and one half times the width of the capture window (currently set at $80\,\mu s$). Let us assume that we were trying to track the phone C_1. From the discussion earlier, we would ideally want to align the start of the capture block with the start of the transmission from C_1. At the moment, this is impossible with the current system as the sampling procedure is started manually by the operator of the DF equipment, but for now, let us assume that it is. The question that still remaining, is what percentage of the samples recorded are erroneous due to overlaps?

A MATLAB script was written to investigate this, and the phones were positioned as indicated in Figure 5.8, C_1 being allocated TS0 and C_2 being allocated TS1. The phones transmit a burst after each TDMA frame in their respective time slots. The simulation parameters were as follows:

Simulation Parameter	Value
Capture window length	$80\,\mu s$
Period between samples	2 ms
Simulation length	0.06 s
No. TDMA Frames	13
No. samples recorded	30

Table 5.2: Simulation Parameters

The results for the simulation are provided below in Table 5.3:

Parameter	Percentage	
Complete hits	TS0 = 15.38	TS1 = 15.38
Time Slot Overlap	15.38	

Table 5.3: Overlap Investigation Results

Comparing the results in Table 5.3 with those in Table 5.2, we can see that the number of unambiguous hits has halved. Similarly the number of overlaps has also increased, which is to be expected given that the amount of overlap has also increased. The results tell us that the occurence of an overlap is equally as probable as a complete hit.

While the overlap appears to be significant it should be noted that the mobile station power levels were not considered, and that while the scenario presented may represent the worst case **time** overlap, it may not necessarily represent the worst case time **and** power scenario.

Because a mobile station can alter its power in steps of 2 dBm during the duration of the call (c.f. Section 2.8.2), the cell phone transmits at a power level that is sufficient to maintain an acceptable channel quality. If C_1 and C_2 were both on the perimeter of the cell, they would be transmitting at roughly the same power (assuming similar propagation losses between the mobiles and the base station). Because C_2 is virtually on top of the DF antenna, the gain of the DF antenna must be kept low so as not to saturate the amplifiers on the front end of the DF antenna. The signal received from C_1 would be very weak by comparison and may go completely undetected which would in fact yield a true DOA for C_2.

For example, let us assume the propagation path between the phones in Figure 5.8 and the base station are identical. Let us also assume that C_1 and C_2 are both on the perimeter of the base station coverage radius (i.e. 35 km away from the base station). If both phones are transmitting a power of 2 W (maximal power transmission for class 4 unit), the power received at the DF antenna according to the power model presented by Garg in Section 4.2.5, $P(R) = 10\gamma logR + x_\sigma$ would be approximately (ignoring the fading term $x_\sigma$and setting $\gamma = 2$ for free space):

$$\begin{aligned} P(R) &= 20log(70km) \\ &\approx 40\,nW \end{aligned}$$

This is a small amount of power, and would most likely be received below the noise floor at the DF antenna. This is problematic particularly if users of the DF equipment are trying to track a phone that is close to the base station, as it would be transmitting very little power compared to a phone on the cell perimeter. Potentially the possibility of changing gain levels between bursts exists, but this would be difficult to implement.

In urban areas, cells are significantly smaller when compared to those in rural areas. For this reason, significant overlap of adjacent time slots on the same frequency at a DF antenna in the cell would probably be insignificant since the timing advances and propagation delays in those cells would be that much smaller. For example, a cell of radius 5 km, would yield an overlap of only $28\,\mu s$.

This concludes the investigation into the significance of TDMA burst overlap. Real GSM datasets were obtained in a parking area using a real DF platform and a number of phones. The results are presented and discussed in the following chapter.

Chapter 6

Real GSM Datasets Analysis

6.1 Introduction

The theory behind GSM and the simulated datasets that would be captured in the field by the DF platform have been discussed in previous chapters. This chapter presents and discussed the datasets that were recorded with the DF platform. The recordings were taken in the car park of company's premises and were done after business hours when there were no cars that would reflect the signals emitted from the phones.

Unfortunately for all the datasets presented in this chapter, only the direction estimates, quality factors and level information were written to disk at the time of recording. Although we were presented with the option of writing the aperture information to disk at the time of recording, the processing time between captures would be increased unpredictably, and the possibility of averaging the aperture information about each GSM carrier (c.f. Section 3.8) was only discovered after the real datasets had been acquired.

6.1.1 Parking Area Geometry

Before discussing the results of the experiments, it would be useful to inspect the area of the parking lot in which the experiments were conducted. This is depicted in Figure 6.1.

The DF antenna was positioned approximately in the centre of the parking lot for all experiments. The area was not really conducive to recording data, as the parking area was surrounded by buildings which would potentially reflect the phone emissions. Pictures of the DF antenna, the equipment rack and the parking lot looking out from Office Building 2 to Office Building 1 can be found in the Appendix.

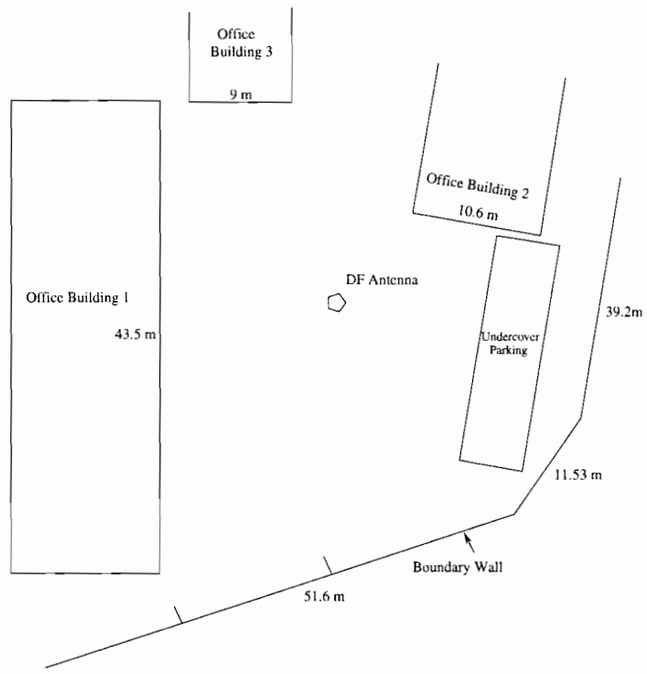


Figure 6.1: Parking Area Geometry

6.1.2 Cellular Providers in South Africa

There are three cellular providers in South Africa. These are "MTN", "Vodacom," and "Cell C." Cell C is a relatively new provider, and was awarded a GSM 1800 licence on the 25th June 2001, allowing them to operate at 1800 MHz. Because they did not have enough infrastructure in place to be self sufficient at the date of launch, Cell C signed a 15-year roaming deal with Vodacom allowing them to make use of Vodacom's allocated frequency spectrum to carry its traffic while construction of new base stations took place [12]. After investigating the signals from a phone with subscribing to the Vodacom network, it seems that in return for the roaming deal, Vodacom are allowed to make use of the 1800 MHz band allocated to Cell C.

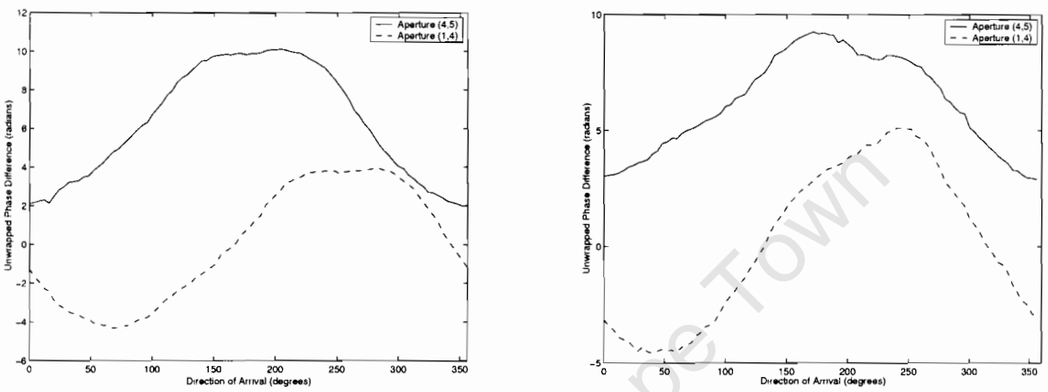
As the DF antenna was tuned to 900 MHz, and because it was not broad enough to cater for both 900 and 1800 MHz bands, only the emissions from phones subscribing to the MTN network were considered. Inspection of the GSM 900 band with the DF platform, reveals that MTN have be allocated the upper half of the spectrum (903 MHz - 915 MHz), and Vodacom and Cell C share the lower half during call initialisation before being transfered to a channel in the 1800 MHz region.

6.1.3 DF Characterisation

Three sets of recordings were performed with two different DF platforms. The DF antenna was characterised for Scenario 1, and again for Scenarios 2 and 3. Recordings for

Scenario 1 were taken using the V3 DF platform. The V5 DF platform was made use of for Scenarios 2 and 3 and was more stable than the initial system. Faster capture rates were also achieved using the V5 system (a guaranteed 2 ms between captures), as opposed to 10 ms between captures for the V3 system.

Because the systems use a different architecture, a characterisation was performed for both systems. The characterisation involved placing the signal generator tuned to 903 MHz approximately 15 m away from the DF antenna at 0°. The characterisation procedure discussed in Section 3.5.2 was then carried out, and the characterisation tables obtained for Scenario 1, and Scenarios 2 and 3 are shown in Figure 6.2 which show the phase differences between two sets of antenna pairs. Note that the spacing between angles (δ) for which the correlation tables were generated was set to 4° in both cases (i.e 90 angular intervals were considered).



(a) V3 platform

(b) V5 platform

Figure 6.2: Inspection of $\phi_n(903\,MHz, \theta)$ for characterisation tables produced for Two DF Systems

The curves look similar to each other, and are approximately sinusoidal and were made use of for the experiments that follow.

6.2 Scenario 1

An initial experiment was conducted on the 7th May 2004 with the V3 DF system, and involved a chordless phone, a single GSM mobile handset, and a signal generator. The chordless handheld phone continuously transmits a narrowband continuous wave signal at a frequency of 915 MHz. The signal generator was used purely as a reference, and was setup at $DOA = 0°$ transmitting a continuous sinusoid at a frequency of 912 MHz. The GSM phone, and the chordless phone were positioned as indicated in Figure 6.3 and traversed a circular path around the DF antenna back to their starting positions over approximately 120 s.

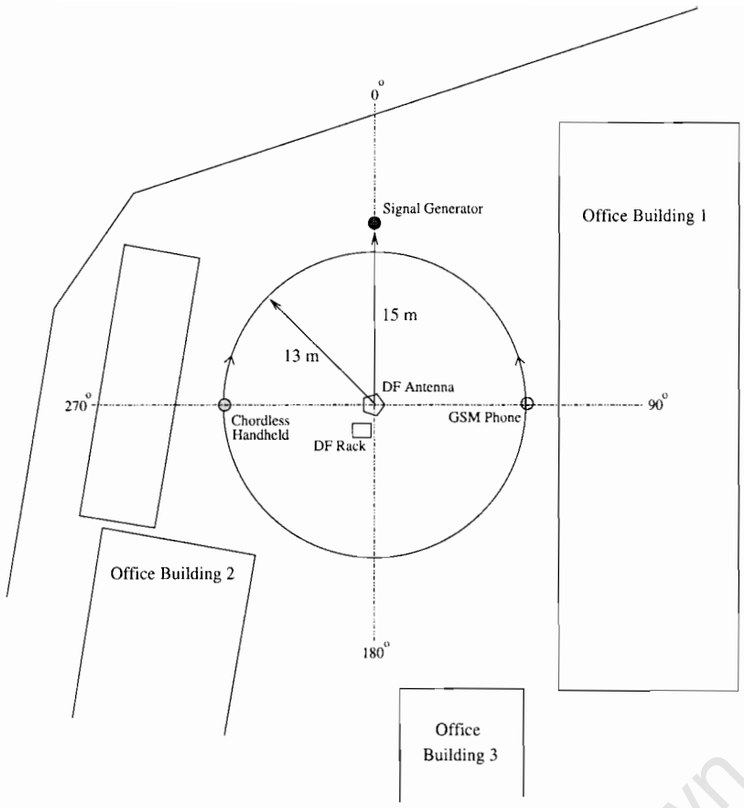


Figure 6.3: Geometry for Scenario 1

6.2.1 Results

Because of the size of the data files that are recorded by the DF platform (of the order of 250 Mbytes), 12 captured frames are compact into one display frame using the method described in Section 4.5.3. The spectogram for this experiment is shown in Figure 6.4. Note that thresholds on the data were set as follows:

Parameter	Value
Signal Level Threshold	-65 dBm
Quality Factor Threshold	83%
Smoothing Kernel Size (pixels)	25x25
Kernel Threshold	80
Kernel Pixel Roll Off Time Axis	15
Kernel Pixel Roll Off Direction Axis	3

Table 6.1: Thresholds for Displaying DOA Estimates for Scenario 1

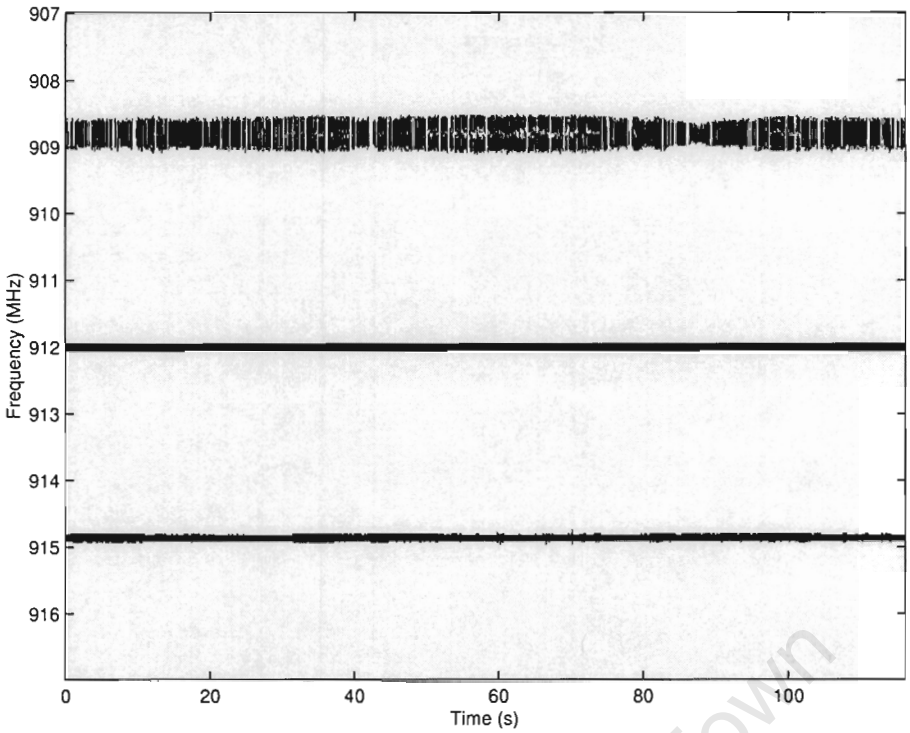


Figure 6.4: Spectogram for Scenario 1

Unfortunately, frequency hopping did not occur for the mobile during this conversation[1]. The mobile can be seen at a carrier frequency of 908.8 MHz (ARFCN = 91). Frequency hopping was possibly disabled because the quality of the traffic channel was sufficient for adequate communication between the base station and the mobile. The reason the cell phone transmission looks virtually continuous, was because the operator of the phone purposefully spoke for as long as possible, trying to avoid pauses. Short gaps are visible though, and are due to the transmitter being inactive as a result of the DTX mode during the conversation. A plot of the DOA estimates before the application of the Gaussian smoothing kernel is shown in Figure 6.5.

[1]Repeated tests showed that frequency hopping did not always take place.

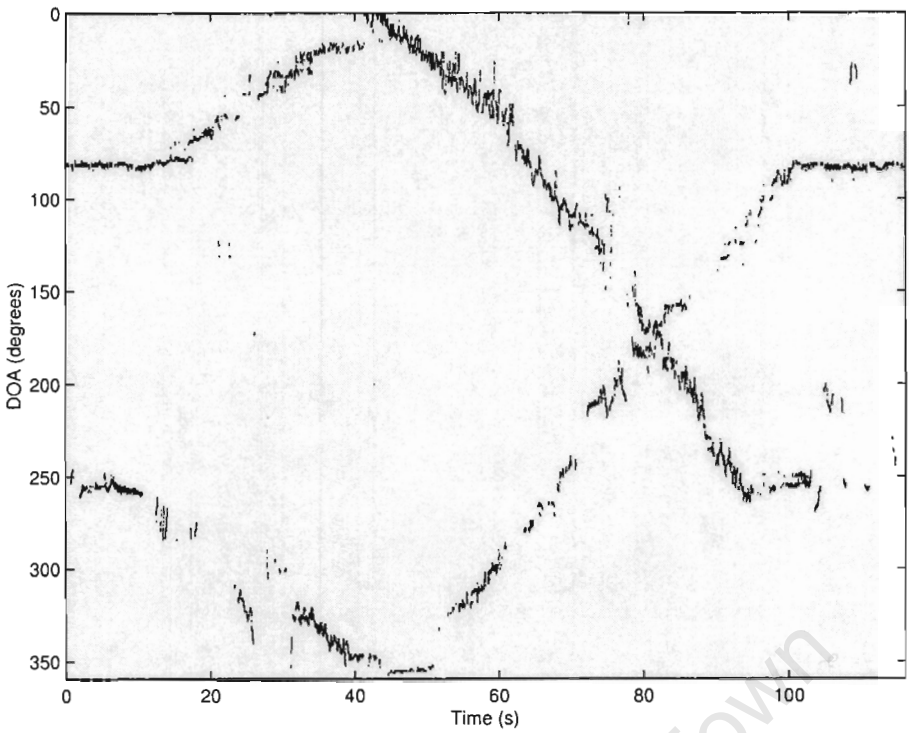


Figure 6.5: DOA Estimation for Scenario 1

It is difficult to distinguish which points belong to the GSM handset, and which points belong to the continuous handheld. To make it easier for the reader to see the motion paths, Figure 6.5 has been plotted again with the known a-priori paths superimposed on top of the plot. This is shown in Figure 6.6.

By knowing the phone paths a-priori, the continuous phone's DOA can be seen starting at approximately 260° and moving through a circle about the DF antenna and back to its original position. The mobile can be observed moving from 90° through a circle around the DF antenna and back to 90° as depicted. They cross twice at approximately 40 s and 80 s as seen in the diagram. The erroneous DOA points at times $t \approx 20\,s$ and $t \approx 110\,s$ for the handheld and the cell phone respectively and are possibly due to reflected signals impinging on the DF antenna at the time of sampling. Because the DF platform was mounted in a square metal rack which was in close proximity to the antenna (2 m away), E-fields could well have been reflected off the sides of the rack onto the DF antenna (a photograph of the rack in close proximity to the antenna can be found in the Appendix). Recall from Section 3.7.2, that for the DF algorithm to work correctly, signals impinging on the antenna must be non-coherent. If the power is strong enough in the coherent signal, an erroneous estimate may arise.

The smoothing kernel described in Section 4.5.3 was applied to the dataset. The result of applying the kernel is shown in Figure 6.7.

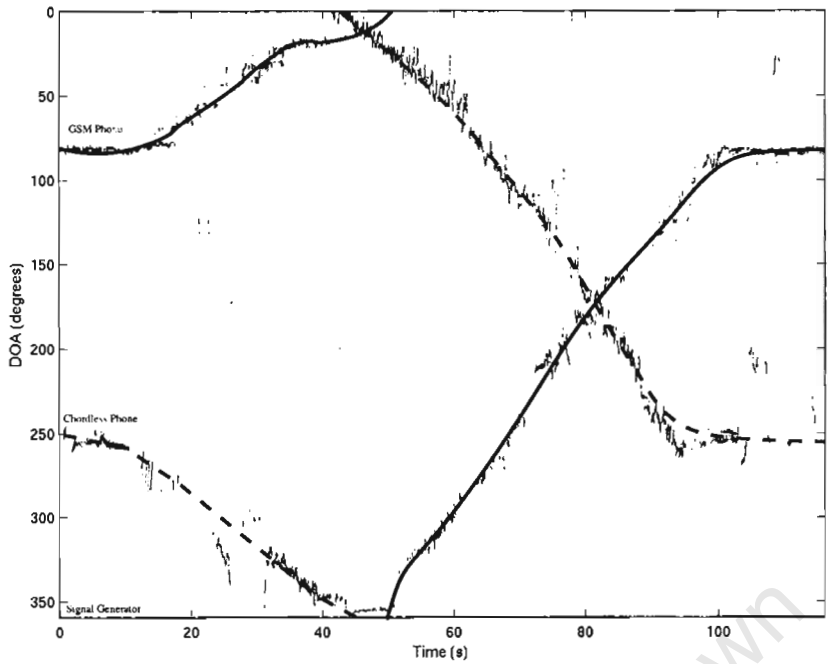


Figure 6.6: Identification of motion paths in dataset for Scenario 1

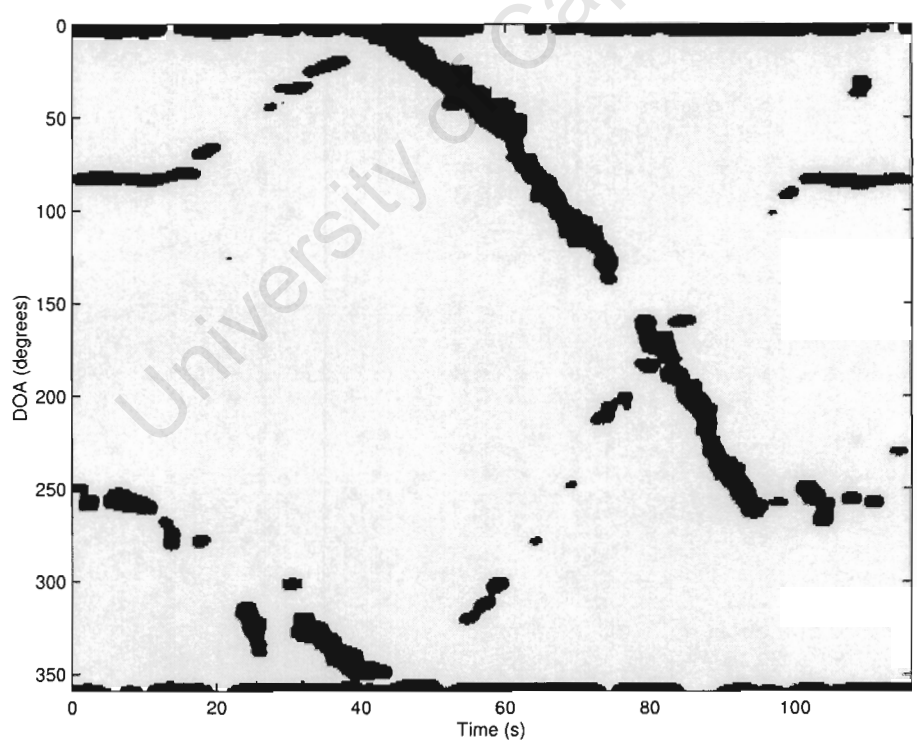


Figure 6.7: DOA Estimates for Scenario 1 when applied to the Smoothing Kernel

As we can see from Figure 6.7, points in close proximity have been fused together, and some of the erroneous DOA estimates have been eradicated, though angular resolution has been reduced. It is interesting to note from this plot, that the density of the dots can

help us to identify which line belongs to which phone. For example, the GSM mobiles data is less continuous than that of the chordless handheld.

6.3 Scenario 2

We have seen from Scenario 1 that if there is only one cellphone in the scene, it may be observed fairly easily. What would happen if we had more than one phone, say for example four? A decision was made to investigate the effects of having up to five mobiles in view of the DF antenna. Unfortunately during the recording session, one of the phones was working intermittently and was not made use of. The V5 platform was used on the 9th of August, 2004 for this Scenario, and Scenario 3.

The approximate starting positions for each of the phones is shown in Figure 6.8 for Scenarios 2 and 3. Each phone traversed a full circle around the DF antenna in the directions indicated by the arrows. Unfortunately, during the recording of the data, some of it was corrupted and had to be discarded. This is because the communication protocol used to connect the DF platform to the recorder that writes each capture to disk is very processor intensive, and as a result, some of the captured packets were discarded in an attempt by the recorder to write the packets to disk at the rate they were being passed to it from the DF platform.

6.3.1 Results

Prior to recording the datasets, it was observed that because frequency hopping was enabled for one or possibly two of the phones, a bandwidth of 10 MHz (the default bandwidth for recording) would be insufficient as the phones occasionally hopped to frequencies outside of the 10 MHz band under investigation. The system bandwidth was thus increased to 20 MHz. This is accomplished on the DF platform by performing two 10 MHz captures one after the other, and then concatenating them to form an effective 20 MHz wide capture. It should be noted that this doesn't directly mimic a true 20 MHz wide capture, as the second 10 MHz band is only captured after the first has been captured and processed.

After selecting a frequency resolution of 25 kHz per frequency bin, each 10 MHz band was captured with a 40 μs window (c.f. Section 4.2.4). The resulting FFT was truncated from 512 points to 400 points to represent a full 10 MHz band. Due to the shorter capture window, the processing period for this 10 MHz band is halved, making it possible to capture a full 20 MHz in the same period of time as that for a 10 MHz band with 12.5 kHz resolution. Basically, by halving the frequency resolution, double the frequency band may be observed in the same amount of time (2 ms per capture). Because the bandwidth of a

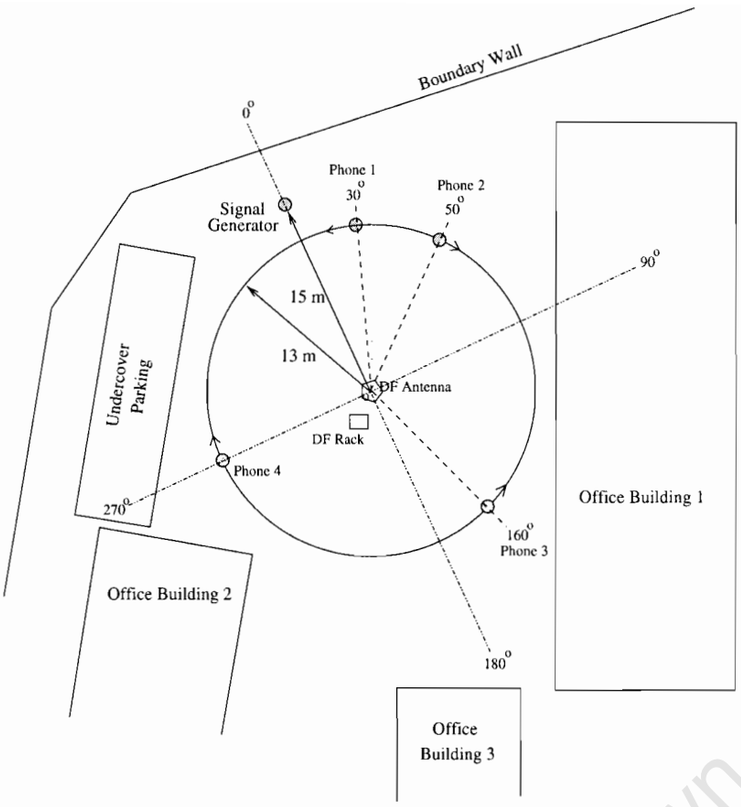


Figure 6.8: Geometry for Scenario 2

GMSK signal is 200 kHz, a frequency resolution of 25 KHz is still a fraction of the 200 kHz.

A spectogram for this experiment is shown in Figure 6.9. Note that, for these datasets, an average of 28 captured frames are compressed into one frame. This means that each display frame represents approximately 56 ms of time. The parameters for the simulation are shown below:

Parameter	**Value**
Signal Level Threshold	-75 dBm
Quality Factor Threshold	80%
Smoothing Kernel Size (pixels)	50x50
Kernel Threshold	6
Kernel Pixel Roll Off Time Axis	13
Kernel Pixel Roll Off Direction Axis	4

Table 6.2: Thresholds for Displaying DOA Estimates for Scenario 2

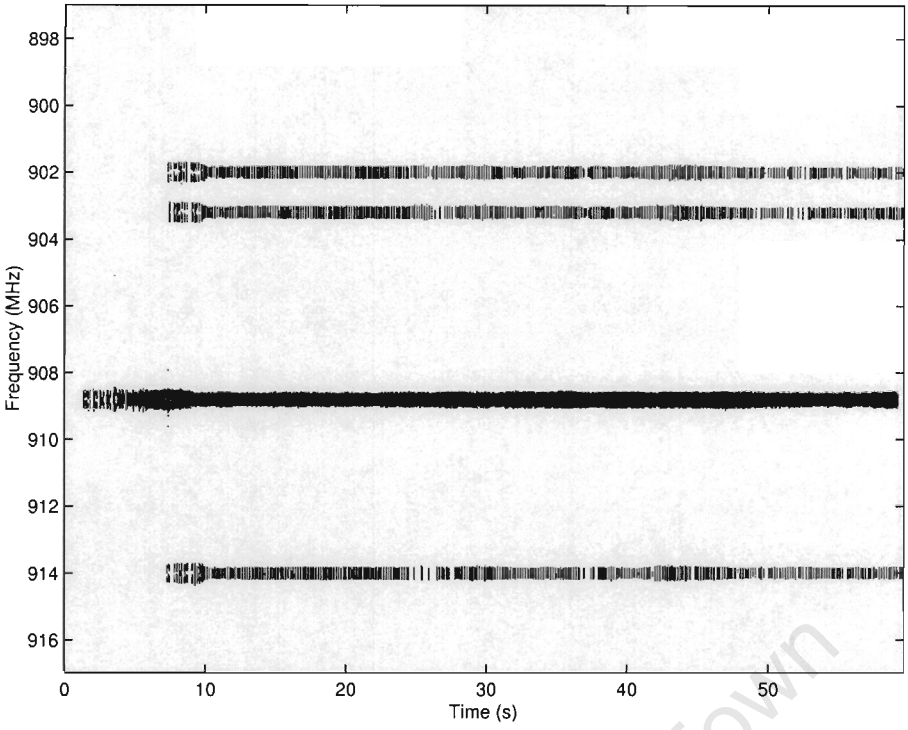


Figure 6.9: Spectogram for Scenario 2

When comparing Figure 6.9 with Figure 6.4, it is clear that more phones are present on the 908.8 MHz (ARFCN = 91) carrier. It is difficult to tell how many phones are actually frequency hopping over the the four RF channels and how many remain solely on the 908.8 MHz carrier. In fact, looking at the spectogram plot visually, it is virtually impossible to determine how many phones are actually present. This information could only be interfered by extracting timing information from the datasets.

Let us now inspect the corresponding direction of arrival plot given by Figure 6.10.

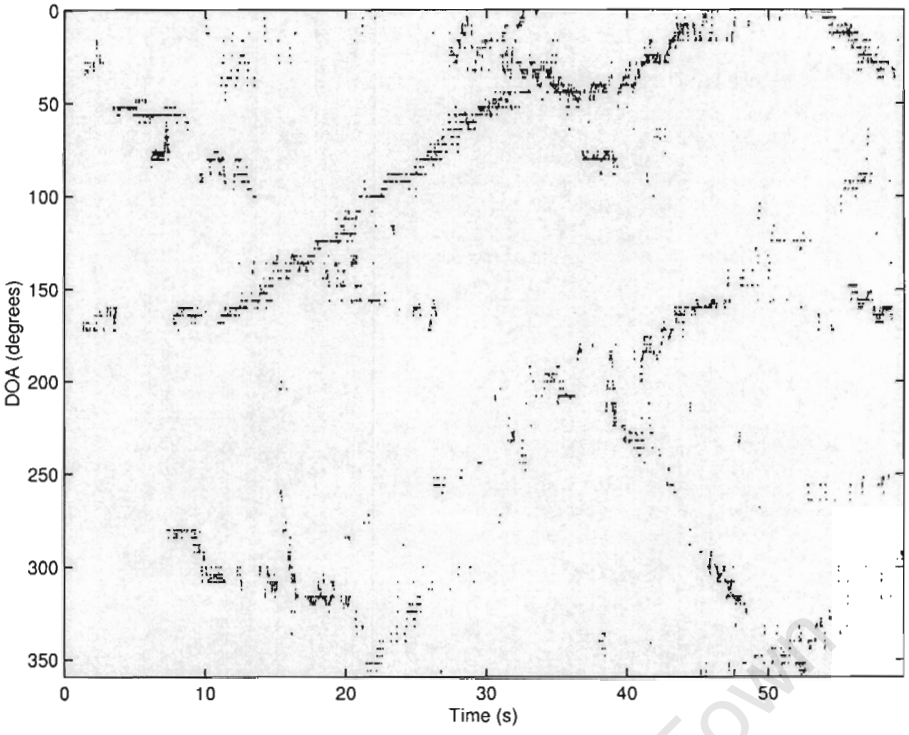


Figure 6.10: DOA Estimation for Scenario 2

We can see that these DOA estimates are not as concentrated around the true DOAs as was observed in the first experiment. This could be as a result of the calibration process where the characterisation table produced using the V3 platform is notably smoother than that produced using the V5 platform (c.f. Figure 6.2). This could be due to the fact that the integration factor (an average of the aperture information recorded at each DOA) was set to a higher value for the first experiment than that of the second.

Once again, at first glance it is visually difficult to draw any conclusions without knowing a-priori the positions of the phones and their motion paths during the recording. However, if we refer back to Figure 6.8, noting the starting positions of the phones and their directions of travel, we can crudely estimate and classify which points belong to which phones over time. This is shown in Figure 6.11.

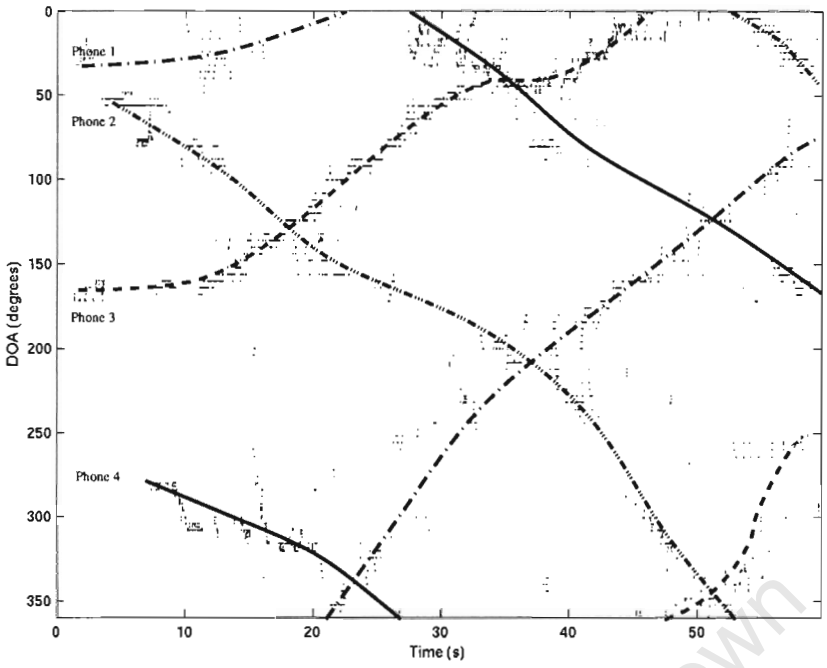


Figure 6.11: Identification of mobile paths in dataset for Scenario 2

Because the standard deviation of the expected DOA points is greater for this experiment than the initial system, the smoothing kernel was made greater in an attempt to group points of close proximity together. The dataset after the application of the smoothing algorithm yielded the results depicted in Figure 6.12.

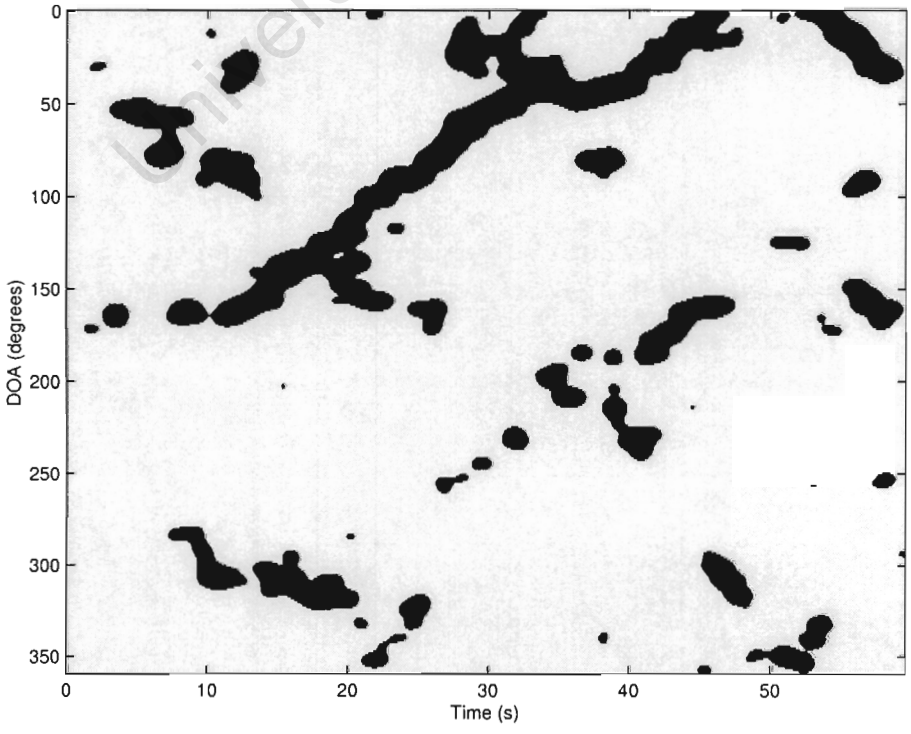


Figure 6.12: DOA Estimates for Scenario 2 when applied to the smoothing kernel

Visually, it is still difficult to see the motion paths of the phones, or how many phones are actually present in the scene. Would it be possible to determine whether the phones had crossed paths or merely met then separated without prior knowledge? This question is addressed in Scenario 3.

6.4 Scenario 3

In the first two scenarios, we considered experiments where the phones crossed each other. What happens now if the phones meet and separate? Will we be able to tell the difference between this, and when the phones actually cross? To investigate this, the four phones were positioned in approximately the same starting positions. Phones 1 and 2 were instructed to cross paths, while phones 3 and 4 were instructed to meet, and then return to their original starting positions. This is depicted in Figure 6.13.

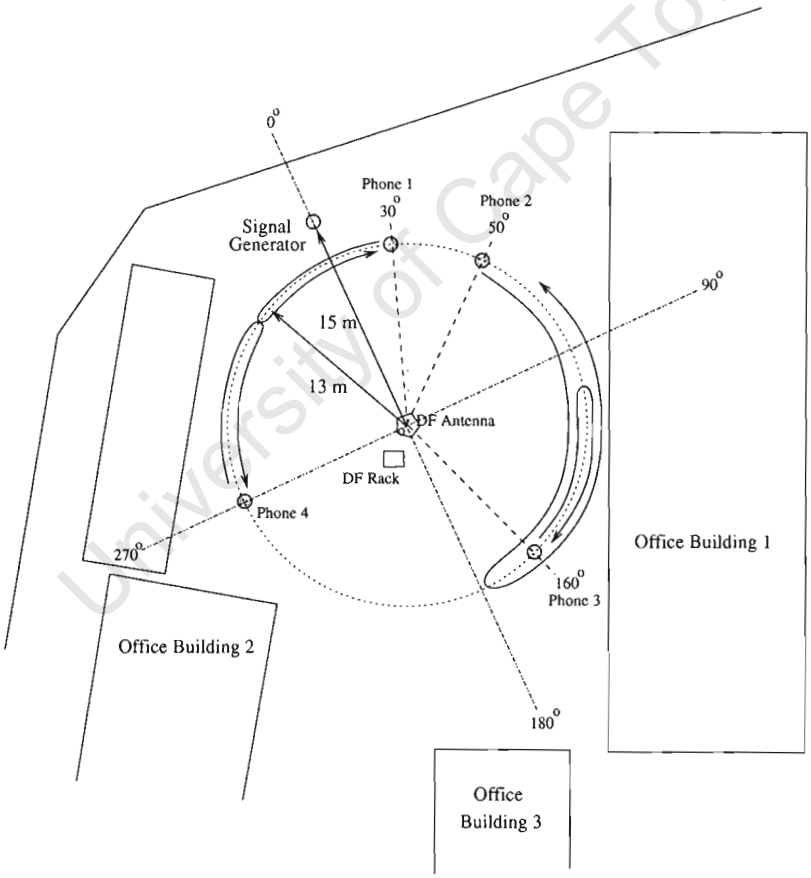


Figure 6.13: Geometry for Scenario 3

6.4.1 Results

We have seen that visually, that spectogram information does not play a significant role in determining the number of phones in the scene (none of the phones were observed to

be frequency hopping for this scenario). As a result, only the DOA data is presented for this scenario in Figure 6.14. Note that as the same characterisation table was used for Scenarios 2 and 3, and as the phones were approximately the same distance away from the DF antenna, the same thresholds used in Scenario 2 are used to process the data for Scenario 3.

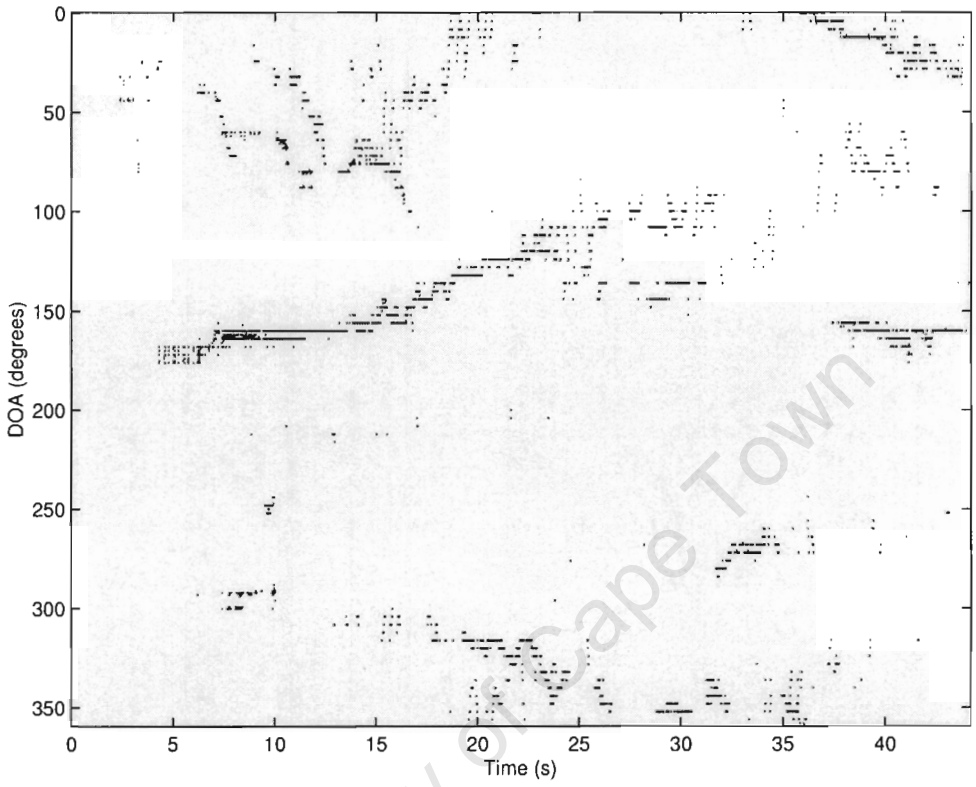


Figure 6.14: DOA Estimation for Scenario 3

Notice again, that it is visually very difficult to infer any information pertaining to the number of phones in the scene, and their directions of motion. Once again, if we make use of the fact that we *knew* how the phones were moving over time, we can see that the majority of the information in the dataset is correct and does correspond to what actually happened during the recording.

If we look carefully at the DOA plot, we can see that there are some erroneous DOA estimates at time $8 < t < 20\,s$. The estimated DOA is approximately at $DOA = 210°$. In addition to the fact that calibration was not optimal, this could also be due to the fact that the DF recording rack was quite close to the DF antenna at the time of recording, causing signals to be reflected off the rack and onto the DF antenna at certain DOAs.

Let us now inspect the data with the application of the smoothing kernel. The results are shown in Figure 6.16.

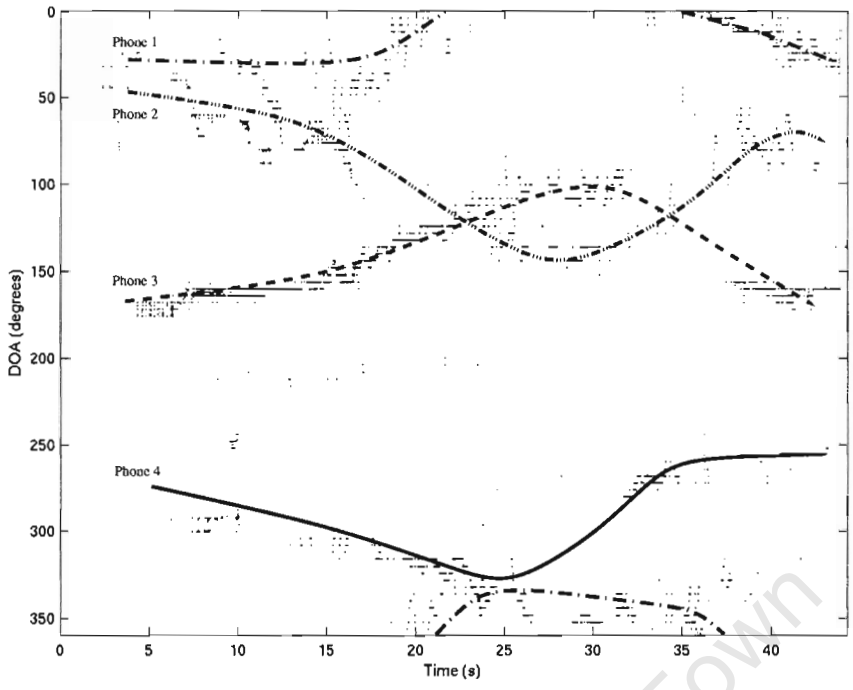


Figure 6.15: Identification of mobile paths in dataset for Scenario 3

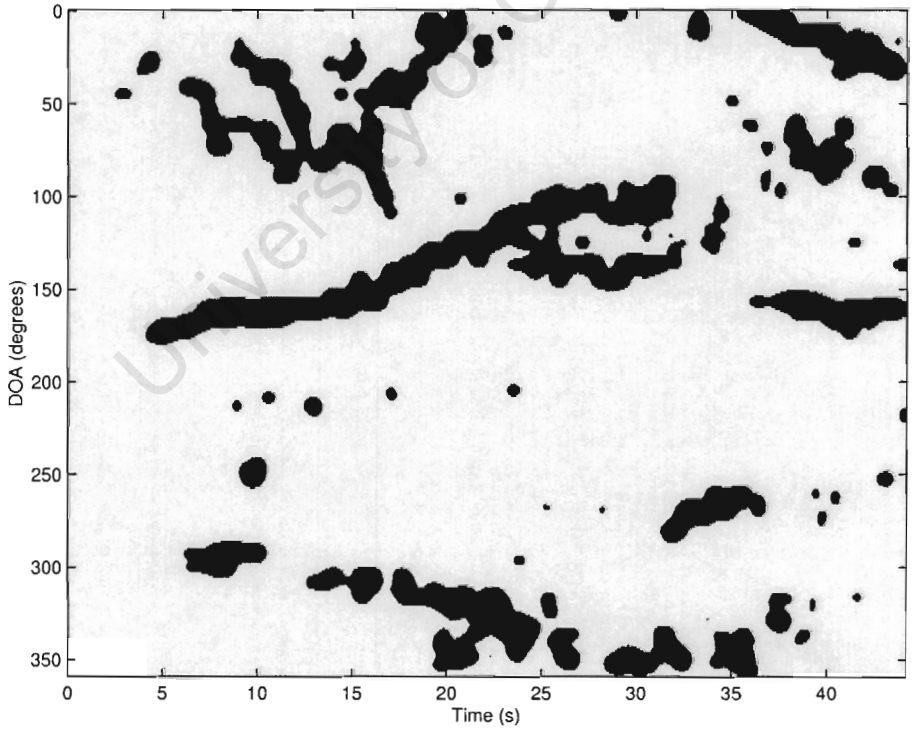


Figure 6.16: DOA Estimates for Scenario 3 when applied to the Smoothing Kernel

From the three scenarios, we can see that visual tracking is indeed very difficult. The application of a smoothing kernel to the data does not really help to identify the motion paths of the phones significantly, even though points in close proximity are fused together.

The data from the first scenario was of a better quality than that for Scenarios 2 and 3. This was because the standard deviation of the estimated DOA points was less, and the quality factors for the estimates were higher, making it easier to identify the paths of the mobiles. More accurate characterisation tables would yield better results, and could be obtained by averaging the captures for each DOA during the characterisation, as the noise would be averaged out.

Three real GSM datasets have been presented and discussed. Conclusions regarding the suitability of the current platform to track mobile phones are covered in the final chapter with recommendations for future work in this area of research.

Chapter 7

Conclusions and Recommendations

An investigation into the suitability of a block sampled, correlative DF platform to detect and track mobile GSM phones was conducted. From the research conducted, I have concluded that the five element DF antenna array will be suitable for detection of mobile phones *depending* on where the DF antenna is going to be used. Simulations conducted in Section 3.7.2, showed that when the DF antenna is exposed to an environment where multipath is an issue, the algorithm breaks down unpredictably. One can conclude from this, that if the DF antenna is positioned in an enclosed environment such as a building or a van where multipath would pose a serious problem, the DF algorithm will break down leading to erroneous DOA estimates. After conducting experiments in the field, we have seen that the DF algorithm will be suitable for estimating the DOAs of GSM handsets.

Because the correlative DF algorithm fails in situations where two signals are simultaneously received on the same frequency, an investigation into the severity of TDMA overlap was conducted. One can concluded from the study that while the potential for a significant time overlap does exist, it should not present a serious problem. It was shown in Section 5.3.2, that for the worst case time overlap, the difference between the power levels for the two cellphones arriving at the DF antenna would be so great, that the one phone farthest away would go undetected. This would have little effect on the DOA estimation for the handset closest to the DF antenna (for the worst possible case of time overlap at the DF antenna). Further investigation should possibly be conducted to explore the tradeoff between the received power levels at the DF antenna, and the amount of overlap at the DF antenna, particularly for cases where the DF platform will be used in urban areas.

At this stage of the research, we have seen from both the simulated, and real datasets, that it is possible to spatially separate out and observe the motion paths for a number of phones in an area, if they are spatially unique. It is difficult to conclude how the DF platform would perform in the field as the datasets that were investigated comprised a number of phones in close proximity to one another and the DF antenna. The DOA changes over time were fairly rapid, which would not necessarily be the case in a real

tracking scenario. For example, it would be very rare for a phone to move in a circle about the DF antenna on a 20 m radius. As a result, the change in DOA over time would be slight, so potential data points missed as a result of the block sampling implementation on the DF platform would not pose a significant problem.

We have seen from simulated datasets, that averaging the aperture information over the GSM carriers reduces the uncertainty of the DOA estimates (c.f. Section 3.8). In the future, aperture information should be stored, and this averaging procedure should be performed before calculating the DOA estimates. We have also seen from the real datasets recorded, that the calibration procedure is crucial to achieving good DOA estimates. For future recordings, a better calibration procedure should be devised, and the aperture information should be averaged at each DOA to average out the white noise.

Future work should focus on the signal processing of the recorded datasets, in particular extracting the timing information from the datasets and classifying which data points belong to which phones. This would not be a trivial task because with the current DF system, it is impossible to know what portion of the TDMA frame is being sampled from sample to sample. With the nature of the current block sampling technique, a particular time slot fades in and out of few of the capture window. It was shown in Section 5.2, that if the period between captures is exactly 2 ms (achievable with the current DF platform), that the sampling pattern repeats every 30 captures ($\frac{60}{13}$ms) due to the modularity of the TDMA/FDMA scheme. Uncertainty arises however because one is never sure what fraction of the timeslot is being sampled with the current system. A particular phone, once allocated a time slot, maintains its time slot for the duration of the call. If there were some way of synchronising the DF sampling *relative* to the GSM network (not necessarily at the start of a TDMA frame), it would be possible from sample to sample to compute which data point belongs to a particular time slot.

At this point, for future tracking, a decision would have to be made as to whether the DF equipment should ideally "lock onto" a particular phone or try to make sense of the signals as captured in the block sampling intervals. The former could be achieved by bandpass filtering the data at positions where phones were detected (thereby isolating each of the phone emissions). The isolated frequency data, would then be inverse transformed back to the time domain. By analysing the time domain waveforms for each capture window, it would be possible to observe when the edge of each phone captured aligns with the start of the capture block, calling this sample instant $t = 0s$. This could be achieved by varying the period between captures until synchronisation occurs. Once synchronisation occurs, it would then be possible to lock onto a particular phone for tracking.

An alternative method would be to try to synchronise with the serving base station by locking onto the *Frequency Correction Channel* (FCCH). This is a downlink channel that is transmitted periodically by all base stations. It conveys information that allows a mobile to tune to the correct frequency of the BTS. It can easily be identified by continuous

sampling equipment as the bursts that are transmitted contain a sequence of logical zeros that produce a frequency shift of 67.7 kHz above the carrier [6]. As these bursts occur in time slot 0, it would be easy to "lock" to time slot 0 for the serving base station. There is still the added complication of propagation delay between the DF antenna and the base station though, and some mechanism would have to be determined that would "undo" the propagation delays between the phones and the base station.

The advantage of opting for this method, is that once aligned with the base station, information present on the *Broadcast Control Channel* (BCCH) could be read and decoded. This information would be useful as it would provide the users of the DF equipment with the frequency set (MA) over which the phones are hopping. In urban areas where the frequency reuse distance is small, it would assist in localising the phones to a particular region as adjacent cells would make use of differing frequency sets. Research has been conducted that addresses the tracking of slowing frequency hopping signals [2, 22].

Once the DOA estimates have been identified as belonging to particular phones, tracking techniques can then be applied. This is an area in which significant research has been conducted and would basically allow for curves to be fitted through the data points in an attempt to track the mobiles. Some of these algorithms approach the problem with a Bayesian frame work [14, 21], whilst Poggio [18] suggests a predictive training methodology for curve fitting. The reader is asked to refer to the papers in the reference list for additional information.

Chapter 8

Appendix

8.1 Configuration Simulation Modules

Appendix 8.1 presents the configurable parameters that are specified in the setup file for the various modules of the simulator.

8.1.1 Base Station Module

Parameter	Description
base_station_position_x	x co-ord of BTS
base_station_position_y	y co-ord of BTS
min_RXLEV_dBm	Minimum power that must be received by a mobile (dBm)
MA	Mobile Allocation
HSN	Hopping Sequence Number
MAIO	Mobile Allocation Index Offset
TS	Time slot allocation for a phone
FN	Initial TMDA frame number
sector_freq	Mobile Allocation Index vector

Table 8.1: Configurable parameters for BTS

8.1.2 Mobile Handset Module

Parameter	Description
no phones	No. of phones in the scene
minimum_talk_time	The minimum talk time for a phone
maximum_talk_time	The maximum talk time for a phone
cellphone_antenna_gain	The gain of the phone amplifier
start_position_x	Initial x co-ord of phone
start_position_y	Initial y co-ord of phone
mid_position_x	Mid point x co-ord of phone
mid_position_y	Mid point y co-ord of phone
final_position_x	Final x co-ord of phone
final_position_y	Final y co-ord of phone
path_time	Time for phone to move from start to finish points
max_power	Maximum phone power

Table 8.2: Configurable parameters for Mobile Handsets

8.1.3 DF Antenna/Receiver Module

Parameter	Description
fs	Sample rate (Hz)
no_antenna_elements	The number of antenna elements
antenna_radius	The DF element radius
antenna_centre_frequency	The centre frequency of the DF antenna
antenna_bandwidth	The bandwidth of the antenna
df_antenna_noise_temperature	Cumulative noise temperature at antenna front end
capture_time	Length of capture window
processing_time	Period of time between capture windows

Table 8.3: Configurable parameters for DF Antenna

8.1.4 Propagation Path Module

Parameter	Description
std_dev_fading	Standard deviation of fast fading (dB)
path loss component	Path loss fading factor

Table 8.4: Configurable parameters for Propagation Path Model

8.2 Pictures of the DF Equipment

8.2.1 Five Element Circular DF Antenna Array

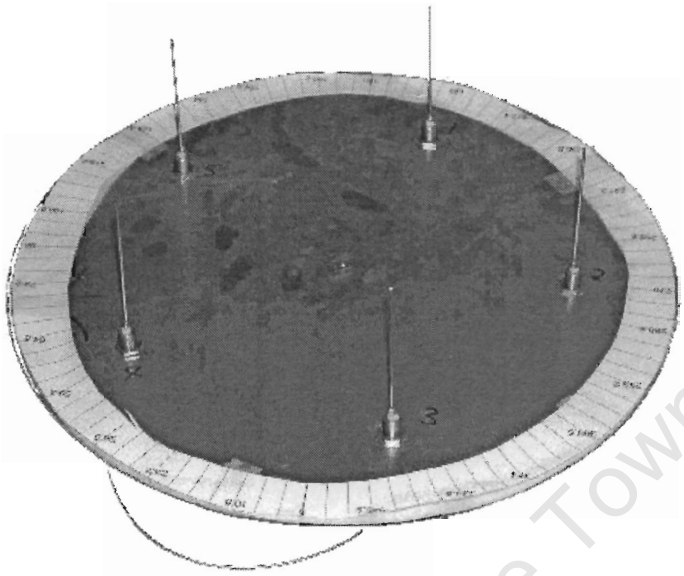


Figure 8.1: Five Element DF Antenna Array

8.2.2 The DF Hardware Platform

Figure 8.2: The DF Platform

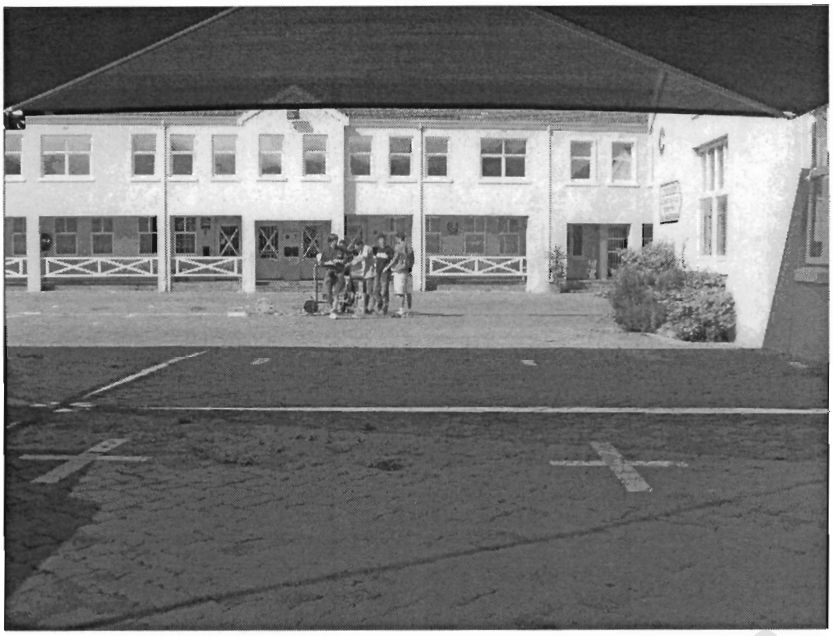


Figure 8.3: View of Building 1 from corner of Building 2

Bibliography

[1] R. Schafer A. Oppenheim. *Discrete-time Signal Processing*. Prentice Hall, 1999.

[2] E.F Deprettere A.N. Lemma, A. van der Veen. Joint angle-frequency esimation for slow frequency hopping signals. Technical report, Delf University of Technology, Netherlands, 1998.

[3] F. Athley. Angle and frequency estimation using sensor arrays. Master's thesis, Chalmers University of Technology, Sweden, 2001.

[4] ETSI Publications, http://www.etsi.org. *GSM Standards*, Various.

[5] M. Viberg H. Krim. Two decades of array signal processing research. Technical report, IEEE Signal Processing Magazine, 1996.

[6] C.Bettstetter. J. Eberspacher, H.Vogel. *GSM Switching Services and Protocols*. John Wiley and Sons, 2003.

[7] C.H. Knapp and G.C. Carter. The generalized correlation method of estimation of time delay. *IEE Trans. Acoustics, Speech and Signal Proc.*, 1976.

[8] J. Kusuma. Parametric frequency estimation: Esprit and music. Technical report, N/A, May, 2002.

[9] W.C.Y Lee. *Mobile Cellular Telecommunications Systems*. McGraw-Hill, New York, 1989.

[10] A. Mehrotra. *GSM System Engineering*. Artech House Publishers, Boston, London, 1997.

[11] B. Mungamuru and P. Aarabi. Enhanced sound localization. Technical report, Univ. Toronto, Toronto, Canada, Dec. 2003.

[12] Cellular Online. *SA's Cell C Launches November 17 2001*. http://www.cellular.co.za/news_2001/110101-cell-c-launch.htm, Nov 2001.

[13] S. Boyd R. Lorenz. Rhobust minimum variance beamforming. Technical report, Information Systems Laboratory, Stanford University, N/A.

[14] D. Ruppert S. Berry, J. Carroll. Bayesian smoothing for measurement error problems. Technical report, Berry Consultants, Texas University, Cornell University, N/A.

[15] T. Van Duzer S. Ramo, J. Whinnery. *Fields and Waves in Communications Electronics*. John Wiley and Sons, 1994.

[16] GSM Cellular Statistics. *Today's GSM*. GSM Association, http://www.gsmworld.com/technology/gsm.shtml, 2004.

[17] F.G Stremler. *Introduction to Communication Systems*. Addison Wesley Publishing Company, 1992.

[18] S. Smale T. Poggio. The mathematics of learning: Dealing with data. Technical report, MIT, University of California, Berkley, 2003.

[19] K. Varma. Time-delay-estimate based direction-of-arrival estimation for speech in reverberent environments. Master's thesis, Virginia Polytechnic Institue and State University, Oct. 2002.

[20] J.E Wilkes V.K Garg. *Principles and Applications of GSM*. Prentice Hall, 1999.

[21] M. Wermen and D Keren. A novel bayesian method for fitting parametric and non-parametric models to noisy data. Technical report, Department of Computer Science, University of Haifa, N/A.

[22] A. Swami X. Liu, N.D Sidriopoulos. Blind multiuser tracking of frequency hopped signals. Technical report, Univ. of Louisville, Univ. of Minnesota, Army Research Lab, N/A.