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

J.R. Lambert-Porter, A.J. Wilkinson

Department of Electrical Engineering
University of Cape Town, South Africa
lmbjon001@mail.uct.ac.za ajw@eng.uct.ac.za

Abstract

Direction Finding (DF) is a process that involves estimating the directions of the arrival (DOA) for propagating wavefronts impinging on an antenna array from arbitrary directions relative to that antenna array.

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 of its popularity on a global scale, 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 paper presents a correlative DF algorithm that is suitable for detecting and inferring DOAs for portable GSM handsets. The algorithm is applied to real datasets obtained in the field, the results of which are presented and discussed together with future work for the tracking of these handsets.

1. Introduction

GSM, is undoubtedly the fastest growing mobile communications system and currently spans over 200 countries. Because of its unprecedented growth, it would be useful for a DF platform to have the ability to infer the DOAs for GSM signals emitted from GSM portable handsets. This paper discusses the feasibility of detecting and tracking portable GSM handsets using a correlative direction finding technique. An initial experiment is described in which blocks of data are captured with a circular 5-element antenna array, using a block sampling DF platform. After suitable signal processing of these datasets, DOA estimates are obtained for each captured block.

In order to fully appreciate the nature of the problem at hand, a brief discussion of the *relevant* aspects of the GSM standard is covered in Section 2. The correlative DOA algorithm is presented in Section 3, with simulated followed by real datasets being presented in Sections 4 and 5. Conclusions and recommendations are presented in Section 6.

2. GSM Architecture

This section serves to briefly summarise the aspects of the GSM standard that are relevant to the problem at hand. The reader is asked to refer to [1, 2, 3, 4] for additional information.

2.1. TDMA / FDMA Access Scheme

GSM 900 uses a combination of a TDMA (Time Division Multiple Access) and FDMA (Frequency Division Multiple Access) schemes and 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 channel is assigned a unique *Absolute Radio Frequency Channel Number* (ARFCN), and is 200 kHz wide (the compactness is as a result of the GMSK digital modulation scheme). In practice the first carrier is discarded to allow for possible out-of-band interference. The uplink portion of the TDMA/FDMA scheme is shown below:

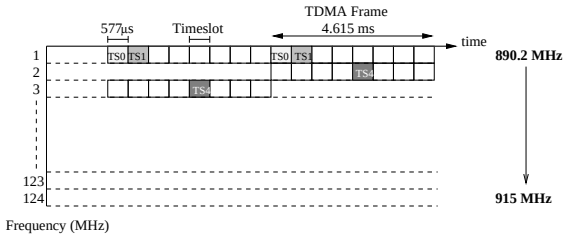

Figure 1: TDMA/FDMA uplink access scheme

Eight timeslots (comprising one TDMA frame) are assigned to a particular carrier on which up to 8 users can transmit and receive information to and from the serving base station. Reception occurs three timeslots after transmission on a carrier in the downlink band which is spaced 45 MHz above the associated uplink channel. 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 22.8 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 the handset undergoes a hand-over from one base station to another).

2.2. Slow Frequency Hopping

To allow for service provision over a large area where the number of subscribers exceeds the number of available channels, GSM allows for the reuse of frequency sets. The 124 available channels are grouped into subsets which are allocated to serving base stations throughout the coverage area. To extend the coverage area, these subsets are reused where co-channel inference between base stations using of the same frequency subset is negligible.

At the start of a call, the base station may instruct the phone to enable slow frequency hopping ($\approx$ 217 Hops/sec). This involves pseudo-randomly changing the transmission frequency at the end of each TDMA frame in an attempt to average the interference over the frequency subsets. This feature is generally

dependent on the quality of the transmission channel between the mobile and the base station.

2.3. Radio Subsystem Link Control

The *Radio Subsystem Link Control* is a bi-directional set of protocols that is responsible for assessing the channel quality, and maintaining synchronisation between the base station and the mobile handset. This information is relayed to the base station approximately twice per second. If the channel quality is insufficient, the base station can instruct the mobile to increase its power level in steps of 2 dBm from 13 dBm up to the maximum power which is dictated by the power class of the mobile (typically 2W). If channel quality is still insufficient, the mobile may re-tune to a new carrier supported by the current base station, or in severe cases, hand-over to a new base station.

2.4. DTX (Discontinuous Transmission Mode)

It has been shown that during a conversation, each speaker speaks approximately 40% of the time. To conserve battery life, a voice activity detector in the handset 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). This means that apart from the channel measurements that are relayed to the base station periodically, the phone essentially transmits nothing apart from the occasional background noise sample.

3. Direction Finding

Direction finding of signals is not a new concept. Since the 1960's, 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 [5, 6]. This section describes a typical, DSP based DF platform that one might use to inspect the GSM band, followed by a correlative DOA algorithm that may be used on such a platform to infer the DOAs for incoming wavefronts.

3.1. Direction Finding Platform

3.1.1. DF Antenna Array

In order to estimate the DOA for an incoming wavefront, a carefully constructed antenna array must be used to capture the signals. Because of the spacing of the antenna elements, the wavefront arrives at each element with a varying time delay that is dependent on its direction of arrival. This time delay, is referred to as the time difference of arrival (TDOA), τ and results in unique set of instantaneous phase differences between the antenna elements for each DOA.

For the purposes of this research, a circular 5 element antenna array was constructed, and is depicted in Figure 2. The elements themselves are tuned monopoles (approximately quarter wavelength) and are positioned onto a ground plate of radius 15 cm. A radial element spacing of 12.5 cm was chosen as a tradeoff between the amount of antenna shadowing, and the DOA ambiguities that arise as a result of the element spacing being too large.

3.1.2. Block Sampling Scheme

Because continuous sampling generates a huge amount of recorded data, a block sampling scheme allows for the storage of recorded datasets recorded over several minutes. Each of the

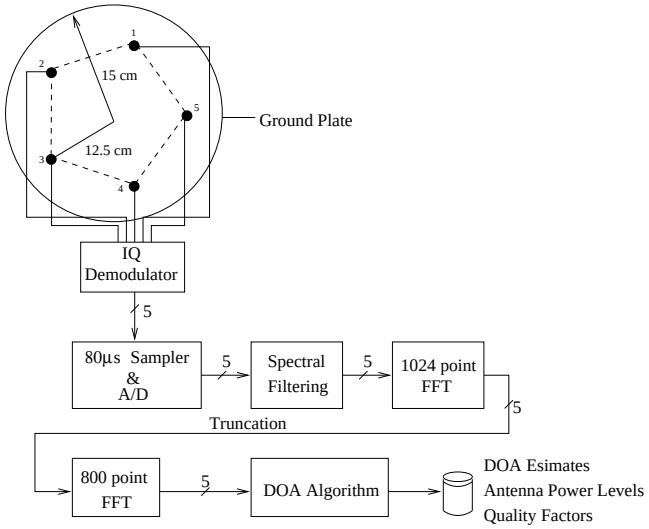

Figure 2: Signal Processing Stages for a typical DF Platform

5 channels of the DF antenna are sampled in parallel at an effective sample rate of 12.8 MHz per antenna channel. Time domain data is sampled in 40 or 80 μs blocks depending on the desired frequency resolution. Table 1 lists the two most commonly used options. Due the FFT computation on the DSPs, the final bandwidth is reduced to 10 MHz for both cases, discarding the aliased edges of the band.

Sample Capture Time	Freq. Resolution	Freq. Bins
40 μs	25 kHz	400
80 μs	12.5 KHz	800

Table 1: Hardware Sampling Options

This dataset for each of the captured channels is then down converted, FFT'd, spectrally filtered using a blackman window (to reduce frequency domain ringing due to the premature truncation of the signal) and finally truncated before being applied to the DOA algorithm. This dataset processing results in a 2 ms delay between successive $80\mu s$ captures. The $40\mu s$ capture window is generally used only when "scanning" the band before switching to an $80\mu s$ capture window for recording.

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. A diagram showing the DF platform as a whole is shown in Figure 2.

3.2. Correlative Direction of Arrival Algorithm

3.2.1. Algorithm Definition

The correlative DOA algorithm correlates the recorded phase differences from every antenna element pair, with a table of precomputed phase differences providing the estimated directions of arrival (and corresponding degree of match) for which the correlation is strongest. In this way, it is very similar to the Generalised Cross Correlation method proposed by Knapp [7]. Before describing the correlation function, the notion of an aperture must be introduced. An aperture is simply an antenna pair.

Because there are 5 antenna elements, there are $n = 1 \ldots 10$ unique apertures which may be formed. To obtain an estimate for the direction of arrival, the captured apertures must be compared with a *characterisation table* $V_n(\omega, \theta)$ of predetermined aperture phase quantities whose phase information should match that of the captured signals at the direction of arrival θ.

The normalised correlation coefficient $C(\omega, \theta)$ is formed, where a perfect match between the recorded data and the characterisation table results in a purely real coefficient equal to 1.

Finally, the factor $Q(\omega, \theta) = \Re e \{C(\omega, \theta)\}$ is used as a measure of the match and will be referred to as the *quality factor* of the estimate where: $-1 \leq Q \leq 1$. The estimated DOA is given where $Q(\omega, \theta)$ attains a maximum for *each* frequency component present in the captured signal.

3.2.2. Characterisation

The process of obtaining $V_n(\omega, \theta)$ is known as *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 is physically rotated from $0^\circ - 360^\circ$. The aperture information is recorded for all apertures at each DOA and are stored in the table before rotating the antenna to the next DOA. In a GSM DF environment, the uplink band is 25 MHz wide, and the centre frequency of which is 903 MHz. The fractional bandwidth is so small (2.8%), that one characterisation table may be used for all the frequencies in this band, rather than computing a new table for each frequency.

Although the characterisation may be done in software thereby generating an ideal table, it is better to obtain the table in the field, as antenna shadowing, and the misalignment of antenna elements is compensated for during the characterisation.

3.2.3. Correlation Coefficient Inspection

To illustrate the correlation coefficients, $C(\omega, \theta)$, two GMSK wavefronts impinging on a simulated antenna similar to that in Figure 2 at frequencies of 898 and 903 MHz were simulated at $DOA = 45^\circ$ and $DOA = 180^\circ$. The SNR was set at 20 dB on each element. An image of $Q(\omega, \theta)$ is shown in Figure 3.

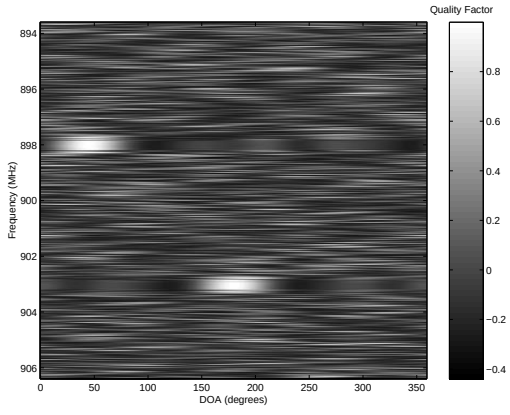

Figure 3: Image of the Quality Factor $Q(\omega, \theta)$ revealing the locations of two incoming signals as two bright spots for which $Q(\omega, \theta) \approx 1$

The DOAs can clearly be seen for the two incoming wavefronts. If the correlation coefficients are plotted for a slice through the 898 MHz carrier, we observe the following in Figure 4.

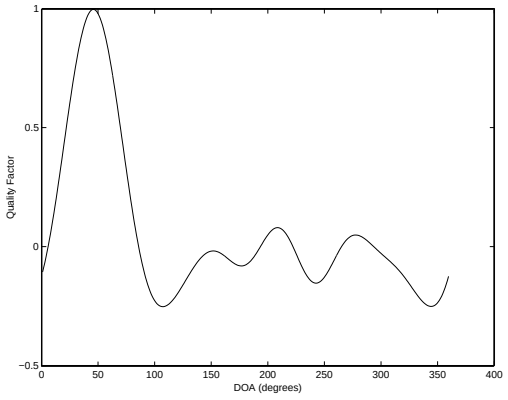

Figure 4: A plot of the correlation coefficients for a slice through the 898MHz carrier

The main peak is correctly observed at $DOA = 45^\circ$ and has a quality factor of 1. Secondary peaks can be seen at $DOA = 210^\circ$ and $DOA = 280^\circ$ as a result of phase ambiguities. In low SNR environments, these peaks can exceed the true peak, and can result in erroneous DOA estimation.

4. GSM Simulator and Display Algorithm

In order to gain a better understanding of the datasets that would be recorded with such a DF platform, a software simulator was developed in MATLAB to model the important characteristics of both the GSM standard (such as frequency hopping, DTX mode, power control etc.), and the DF platform (such as the block sampling nature of the platform, the capture times, and capture bandwidths etc).

Recall, that the platform is typically configured to sample $80\,\mu s$ of data every 2 ms and that a GSM TDMA 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, realigning with the edge of TS0 after 30 TDMA frames. This is more clearly shown in Figure 5 where TS0 can be seen moving in and out of the capture window.

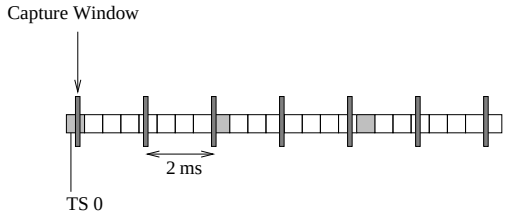

Figure 5: Block Sampling of Timeslots

This moving in and out results in short gaps 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 sampled is not constant and large gaps may appear in the dataset. A high level simulator diagram is shown in Figure 6. The display algorithm will be discussed shortly after a simulated scenario has been presented.

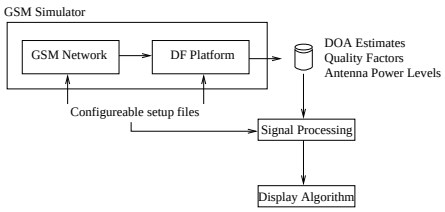

Figure 6: Overview of Simulator Flow Diagram

In order to test the simulator, a scenario was simulated, the details of which are discussed shortly.

4.1. Simulation 1

To test the simulator, GSM data were simulated for approximately 138s (30000 TDMA frames). Three phones (maximum power transmission = 2W) were assigned 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 is illustrated in Figure 7. Pseudo random frequency hopping over the carriers was activated for the simulation. During the course of the simulation, phone 1 and phone 3 moved along the lines indicated so that the output of the DOA could be verified. Phone 2 remained stationary.

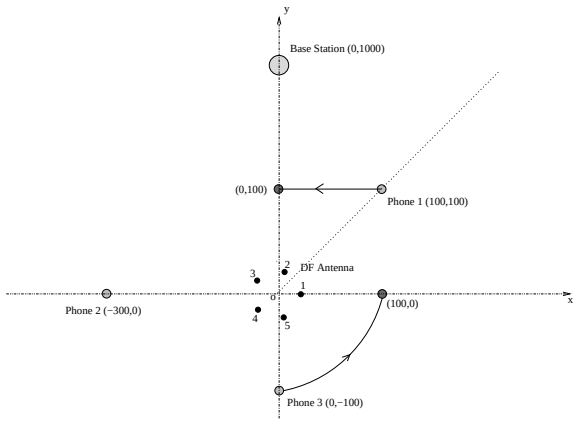

Figure 7: Geometry for Scenario 1

4.1.1. Results

Two plots can be generated from the data recorded, a spectogram, and a estimated DOA plot. Because of the size of the files written to disk (approximately 150 MB for 140 s of data), either every nth captured frame can be displayed, or alternatively n sequential captures can be compressed into one display frame. The danger in displaying every nth frame, is that potentially good DOA estimates can be skipped over. Because of this, the first option will be ignored, and we will turn our attention to the second method.

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. After setting a level threshold exceeding -30 dB, and quality factor exceeding 95%, the following spectogram and DOA plot were observed in Figure 8 and Figure 9 respectively.

Each vertical line of the spectogram and DOA plot constitutes the data from 67 captured frames. It is difficult to identify from the spectogram plot how many mobiles are present in the area, or if they are actually hopping. The only useful information that an observer can infer from this plot, is the number of carriers over which the phones are potentially hopping.

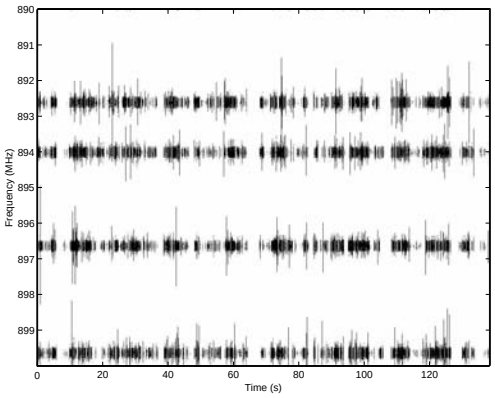

Figure 8: Spectogram for Simulation 1

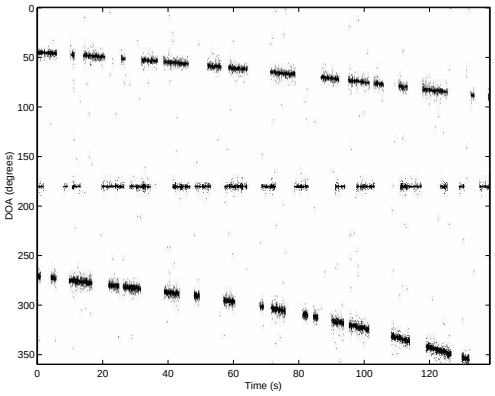

Figure 9: DOA for Simulation 1

We can clearly see the tracks of the three phones in the DOA plot. If we look carefully at the DOA plot, we can see that 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). We can also see that several data points concentrate around the true DOA. The spread is due to the fact that DOA estimates are corrupted by noise. If the algorithm could incorporate the GSM frequency information (in particular the known bandwidth of the GMSK signals, and the GSM carrier frequen-

cies), better DOA estimates could be computed by averaging the aperture information over the GMSK band, as the phase information for a particular aperture should be virtually identical across the 200 kHz bandwidth of a GMSK transmission.

For each GSM carrier location ω_c, the averaged aperture information for N values across a 200 kHz wide GMSK waveform is defined as:

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

where $\Delta\omega$ represents the FFT resolution and $S_n(\omega)$ refers to the nth captured aperture. For a 12.5 kHz resolution, $N = \frac{200}{12.5} = 16$.

The resulting DOA vs time image is shown in Figure 10 and shows a definite improvement over Figure 9. The speckle has been reduced, and the points around the true DOA have converged.

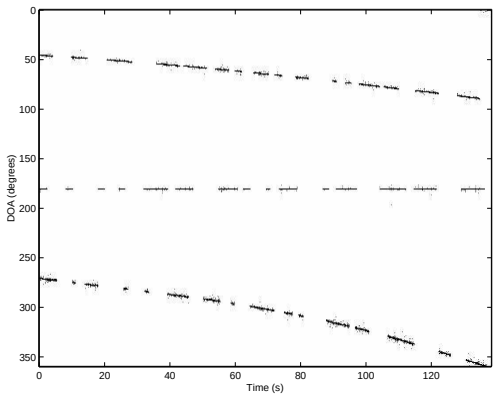

Figure 10: Improved DOA Estimates for Simulation 1

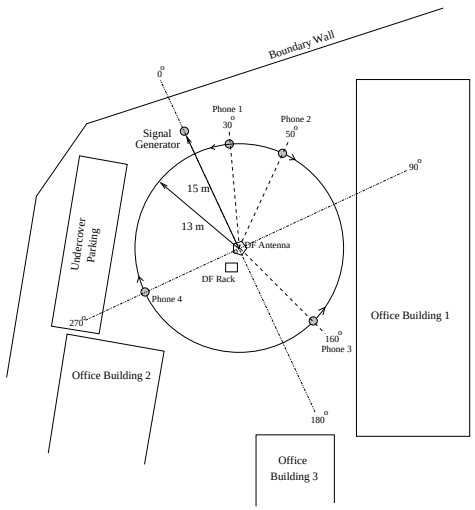

Figure 11: Geometry for Real Data Set Acquisition

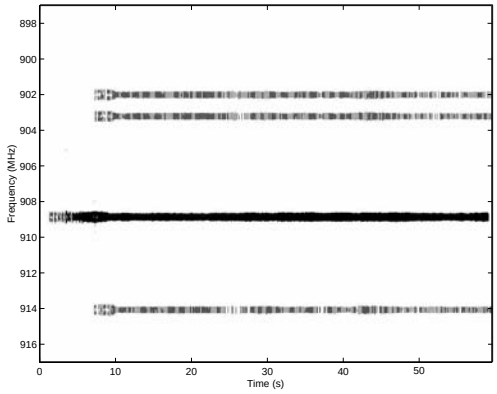

Figure 12: Spectogram for Real Dataset

5. Real Dataset Analysis

In order to inspect real data sets, recordings of cellphone emissions were taken in an empty car park using a wide band DF platform capable of a 20 MHz bandwidth capture every 2 ms (basically two concatenated 10 MHz captures, of 25 kHz frequency resolution). Four MTN network phones were made use of in the experiment, and the geometry is shown in Figure 11. The operator of each phone was instructed to walk in a complete circle about the DF antenna as shown. A signal generator was positioned at 0° for characterisation, but was turned off at the start of the experiment. Hardware limitations did not permit both aperture information and direction information to be stored, and in this first experiment, only direction information was stored.

5.1. Results

Data were displayed with a level threshold of -70 dBm and a quality factor threshold of 80%. The following was observed for the spectogram in Figure 12 and the DOA plot in Figure 13.

It was observed that four RF channels were active, but with a higher concentration on the 908.8 MHz carrier (ARFCN=91). In fact, visually it is virtually impossible to determine how many phones are actually present via inspection of the spectogram alone. Note that the results illustrated in Figure 13 did not undergo the aperture averaging operation. This also presents an extreme case, as most phones would not change angle this quickly as a function of time.

Cellphone tracks are visible, however it is difficult to determine which points belong to which phones without knowing a-priori, the positions of the phones and their motion paths during the recording. However, if we refer back to Figure 11, noting the starting positions of the phones and their directions of travel, we can estimate and classify which points belong to which phones over time. This is shown in Figure 14.

It is predicted that if the averaging operation mentioned in Section 4.1.1 is applied to the aperture data before computing the directions of arrival, the uncertainty in the estimates will be reduced significantly.

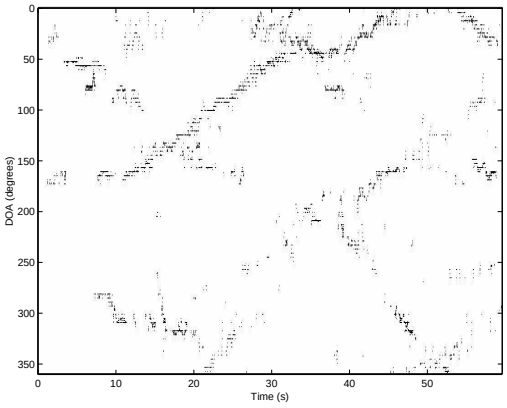

Figure 13: DOA Estimation for Real Dataset

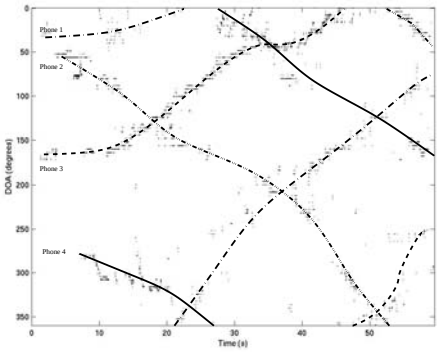

Figure 14: Identification of mobile paths in dataset for Scenario 2

6. Conclusions and Recommendations

From the research conducted thus far, it is concluded that the 5 element DF antenna array will be suitable for detection of mobile phones. At this stage of the research, we have seen 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 was also observed that by averaging the aperture information around the GSM carriers, improved DOA estimates could be obtained, although this has not yet been implemented on the real data.

The reader should note that conditions were not ideal for the recording of the real datasets. The surrounding buildings would have caused reflections, and in addition, characterisation was performed by mounting the DF antenna on a stepper motor. Work should be done on refining the calibration procedure, in particular averaging the apertures for a each DOA, to average out noise. Currently, the timing information from the datasets has not been explored. If the DF block sampling technique is aligned 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.

7. Acknowledgements

We would like to thank Peralex Electronics, Cape Town, South Africa for financial support and for providing access to GEW direction finding equipment without which this research would not have been possible. The NRF is also acknowledged for their support via the THRIP programme.

8. References

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

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

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

[4] J. W. V.K Garg, *Principles and Applications of GSM*. Prentice Hall, 1999.

[5] 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.

[6] M. V. H. Krim, "Two decades of array signal processing research," tech. rep., IEEE Signal Processing Magazine, 1996.

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