

**UNIVERSITY OF CALGARY**

**Super Resolution of Discrete Arrivals in a Cellular Geolocation System**

**by**

**Andrew Louis Borsodi**

**A THESIS**

**SUBMITTED TO THE FACULTY OF GRADUATE STUDIES  
IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE  
DEGREE OF MASTER OF SCIENCE**

**DEPARTMENT OF ELECTRICAL AND  
COMPUTER ENGINEERING**

**CALGARY, ALBERTA**

**APRIL, 2000**

**© Andrew Louis Borsodi 2000**



National Library  
of Canada

Acquisitions and  
Bibliographic Services

395 Wellington Street  
Ottawa ON K1A 0N4  
Canada

Bibliothèque nationale  
du Canada

Acquisitions et  
services bibliographiques

395, rue Wellington  
Ottawa ON K1A 0N4  
Canada

*Your file* *Votre référence*

*Our file* *Notre référence*

The author has granted a non-exclusive licence allowing the National Library of Canada to reproduce, loan, distribute or sell copies of this thesis in microform, paper or electronic formats.

The author retains ownership of the copyright in this thesis. Neither the thesis nor substantial extracts from it may be printed or otherwise reproduced without the author's permission.

L'auteur a accordé une licence non exclusive permettant à la Bibliothèque nationale du Canada de reproduire, prêter, distribuer ou vendre des copies de cette thèse sous la forme de microfiche/film, de reproduction sur papier ou sur format électronique.

L'auteur conserve la propriété du droit d'auteur qui protège cette thèse. Ni la thèse ni des extraits substantiels de celle-ci ne doivent être imprimés ou autrement reproduits sans son autorisation.

0-612-49670-8

**Canada**

## Abstract

A method to determine a cellular subscriber's location which utilizes the digital mode of the IS-54-B air-interface standard, and subsequently the IS-136 air-interface standard, is presented. Time-of-arrival (TOA) estimates are made by correlating the cellular mobile's transmit burst message; either normal traffic or shortened bursts, with the cellular mobile's assigned time-slot synchronization word. The resolution of the time estimates are further improved by employing super-resolution processing, which helps mitigate multipath effects incurred by the mobile radio channel. The polynomial variant of Schmidt's MUSIC algorithm, root-MUSIC, is utilized in the processing method. The super-resolved TOA values are used in conventional multilateration algorithms to obtain two-dimensional position estimates. An overview of super-resolution processing by previous researchers at the University of Calgary is provided. Computer simulations are conducted on wideband signals, including indoor channel measurements, and air-interface signaling used for the North American digital cellular system.

## Acknowledgments

The author is deeply indebted to his supervisor, Dr. Michel Fattouche, who has been a friend, and mentor throughout the course of this research. The author wishes to thank him for his support, encouragement, and tremendous patience for my literary motivation over the years. The author gratefully acknowledges the financial support of this research, provided in part, by Telecommunications Research Laboratories (*TRLabs*) and the Department of Electrical and Computer Engineering. Thanks and recognition also go to the staff and research colleagues at both *TRLabs* and the Department of Electrical and Computer Engineering for their support and camaraderie over the years, and to Lisa Dumont for insightful discussions on super-resolution processing. A special thanks goes to Thomas Borsodi, for helping edit and improve the quality of this thesis, and the many enlightening discussions had over coffee sessions.

*To my parents, who encouraged knowledge and wholly educated their children  
with all the difficulties they had, I dedicate this \$0.02.*

## Table of Contents

Title Page .....	i
Approval Page .....	ii
Abstract .....	iii
Acknowledgments .....	iv
Dedication .....	v
Table of Contents .....	vi
List of Tables .....	ix
List of Figures .....	x
List of Symbols .....	xiii
Chapter 1: Introduction .....	1
1.1 Motivation of CMRS Navigation .....	1
1.2 Existing Navigation Technologies .....	6
1.3 Signal Parameter Resolution .....	10
1.4 Thesis Overview .....	11
Chapter 2: Eigenvector Projection Estimators .....	14
2.1 Super-Resolution .....	14
2.2 The MUSIC Algorithm .....	16
2.3 The Root-MUSIC Algorithm .....	25
2.4 AOA Super-Resolution Processing of Radio Frequency Signals .....	31
2.5 TOA Super-Resolution Processing of Radio Frequency Signals .....	35
2.6 The SCID Method .....	36
2.7 SCID Architecture Considerations .....	43
2.7.1 Code Compression .....	43
2.7.2 Sample Reduced Correlation Sequence .....	44

2.7.3	Mode Estimation . . . . .	45
2.7.4	Candidate Roots . . . . .	46
2.7.5	DC Estimation . . . . .	50
2.8	The Modified SCID Method . . . . .	50
2.9	Modified SCID Architecture Considerations . . . . .	51
2.9.1	Mode Estimation . . . . .	52
2.9.2	Candidate Roots . . . . .	52
2.9.3	Bias Estimation . . . . .	54
2.10	TOA Estimation of Maximum Length Shift-Register Sequences . . . . .	55
2.11	Indoor Baseline Estimation . . . . .	63
 Chapter 3: Concepts of North American Cellular and Geolocation Systems . . . . .		69
3.1	North American Cellular Radio Architecture . . . . .	69
3.2	IS-54-B Air - Network Interface . . . . .	75
3.3	North American Digital Cellular Radio (IS-54-B) . . . . .	80
3.4	RECC Time-of-Arrival processing . . . . .	83
3.5	Subscriber Identification . . . . .	91
3.6	IS-54-B Time-of-Arrival Processing . . . . .	93
 Chapter 4: NADC Geolocation . . . . .		102
4.1	Digital Cellular Radio Positioning . . . . .	102
4.2	Path Loss Models . . . . .	103
4.3	TOA Multilateration . . . . .	107
4.4	Matrix Conditioning and Algorithm Stability . . . . .	110
4.5	Direct TOA Substitution Using Circular Format . . . . .	115
4.6	Simulation of Two-Dimensional IS-54-B Positioning . . . . .	119
4.7	Master Time Reference Errors . . . . .	126

<b>Chapter 5: Conclusions</b> .....	<b>128</b>
<b>5.1 Summary of the Thesis</b> .....	<b>128</b>
<b>5.2 Proposed Topics of Further Research and Other Thoughts</b> .....	<b>129</b>
<b>5.2.1 Reliability</b> .....	<b>130</b>
<b>5.2.2 Signal Interception</b> .....	<b>134</b>
<b>5.2.3 Network Integration</b> .....	<b>134</b>
<b>5.3 Positioning of Personal Communication Systems</b> .....	<b>137</b>
<b>References</b> .....	<b>138</b>
<b>Appendix A: Overhead Messages</b> .....	<b>146</b>

## List of Tables

Table 2.1	Magnitude of Polynomial Coefficients	49
Table 2.2	SCID Estimated Baselines	66
Table 2.3	mSCID Estimated Baselines	67
Table 2.4	Mean Baseline Estimates	68
Table 3.1	Modulation Indexes for AMPS	70
Table 3.2	RECC Data Fields	78
Table 3.3	Mobile Station Power Levels	79
Table 3.4	Differential Phase Encoding	82
Table 3.5	Static Data Precision and Accuracy Measurements	87
Table 3.6	Time Slot Synchronization Sequences (normalized by $\pi/4$ )	95
Table 4.1	LS UTM Coordinates	115
Table A.1	Station Class Mark	146
Table A.2	Abbreviated order and Order Qualification Codes	147
Table A.3	Mobile Phone Class Identifier	148

## List of Figures

Figure 1.1	Annual cellular 911 calls in the USA . . . . .	4
Figure 2.1	Frequency estimator for the two source example at 20 dB SNR, where the MUSIC Null spectra has been normalized . . . . .	22
Figure 2.2	Polynomial zeros for the two source frequency estimation example at 20 dB SNR . . . . .	27
Figure 2.3	Polynomial zeros for the two source frequency estimation example at 20dB SNR, reciprocal zeros are not illustrated . . . . .	28
Figure 2.4	Frequency estimator and polynomial zeros for the two source example at 15 dB SNR, reciprocal zeros are not illustrated . . . . .	29
Figure 2.5	Line of bearing accuracy . . . . .	34
Figure 2.6	Line of bearing accuracy on two-dimensional positioning . . . . .	34
Figure 2.7	Baseband equivalent model of the TOA estimator . . . . .	37
Figure 2.8	Polynomial zeros of TOA estimator for two sources at 20 dB SNR . . .	41
Figure 2.9	Block diagram of a real-time SOI interceptor . . . . .	43
Figure 2.10	Illustration of harmonic properties of cross-correlation sequences . . . .	44
Figure 2.11	Polynomial zeros of TOA estimator for two sources at 20 dB SNR, where $\alpha_1/\alpha_2 = 0.1$ (i.e. -20 dB) . . . . .	47
Figure 2.12	Polynomial zeros of TOA estimator for two sources at 20 dB SNR, where $\alpha_1/\alpha_2 = 0.1$ . . . . .	53
Figure 2.13	LOS TOA error for single source case, with error normalized to the symbol period . . . . .	56
Figure 2.14	Standard deviation of LOS estimation, normalized to the symbol period . . . . .	57
Figure 2.15	LOS TOA error for $\Delta\tau_{12} = T_{symbol}/2$ . . . . .	58
Figure 2.16	Non-LOS TOA error for $\Delta\tau_{12} = T_{symbol}/2$ . . . . .	59
Figure 2.17	SCID LOS estimation error for varying $\Delta\tau_N$ . . . . .	60
Figure 2.18	mSCID LOS estimation error for varying $\Delta\tau_N$ . . . . .	61

Figure 2.19	mSCID/b LOS estimation error for varying $\Delta\tau_N$ .....	61
Figure 2.20	SCID LOS TOA error for varying LOS magnitude relative to the multipath component, with $\Delta\tau_{12} = T_{symbol}/2$ .....	62
Figure 2.21	mSCID LOS TOA error for varying LOS magnitude relative to the multipath component, with $\Delta\tau_{12} = T_{symbol}/2$ .....	63
Figure 2.22	IRIS transmitter - receiver block diagram .....	64
Figure 3.1	Wireless and wired connectivity of CMRS .....	70
Figure 3.2	Frequency allocation for Enhanced AMPS .....	72
Figure 3.3	Illustration of hexagonal cell and practical cell having uniform received signal strength at the cell boundaries .....	73
Figure 3.4	Illustration for frequency reuse plan of $N = 7$ .....	73
Figure 3.5	Illustration of cochannel distance for $N = 7$ .....	74
Figure 3.6	Mobile Station - Base Station (RECC) message format .....	76
Figure 3.7	RECC word formats .....	77
Figure 3.8	Constellation diagram for $\pi/4$ - DQPSK modulation .....	81
Figure 3.9	Block diagram of $\pi/4$ - DQPSK modulator .....	81
Figure 3.10	Block diagram of RECC Listening Station equipment .....	83
Figure 3.11	Simulated horizontal position accuracy for given HDOP .....	86
Figure 3.12	Base Station - Mobile Station (FOCC) message format .....	88
Figure 3.13	RECC collision .....	89
Figure 3.14	RECC collision occurring before 56 bits are transmitted .....	89
Figure 3.15	Failed RECC access attempt, determined after 104 bits .....	90
Figure 3.16	Mobile Station - Base Station (RDTC) slot format .....	93
Figure 3.17	Base Station - Mobile Station (FDTC) slot format .....	93
Figure 3.18	Shortened Burst format .....	94
Figure 3.19	Normalized cross correlation sequences for time slot 3 and CDVCC 1 (noiseless case) .....	96
Figure 3.20	Standard offset for digital traffic channels with no timing advance ...	98
Figure 3.21	General receiver for BP activity detection .....	99
Figure 3.22	BP architecture operating characteristics for NADC SOI .....	100

Figure 4.1	Illustration of typical normalized CIR delay profiles . . . . .	106
Figure 4.2	Geometry of AVM system . . . . .	107
Figure 4.3	Illustration of circular format location algorithm . . . . .	116
Figure 4.4	Listening Station distribution for position estimation . . . . .	120
Figure 4.5	Position error distribution for normal RDTC bursts . . . . .	122
Figure 4.6	Position error distribution for shortened bursts . . . . .	123
Figure 4.7	Constrained ( $HDOP \leq 3$ ) position error distribution for normal RDTC bursts . . . . .	124
Figure 4.8	Constrained ( $HDOP \leq 3$ ) position error distribution for shortened bursts . . . . .	125
Figure 4.9	Constrained ( $HDOP \leq 3$ ) position error distribution for averaged normal RDTC bursts . . . . .	126
Figure 4.10	Constrained ( $HDOP \leq 3$ ) position error distribution for shortened bursts and $\sigma_t = 100$ ns . . . . .	127

## List of Symbols

$\mu\text{s}$	microsecond
ADC	analog to digital converter
AFG	arbitrary function generator
AGT	Alberta Government Telephones
AMPS	Advanced Mobile Phone Service
ANI	automatic number identification
AOA	angle of arrival
APCO	Association of Public Safety Communications Officials International
ASIC	application specific integrated circuit
AT&T	American Telephone and Telegraph
AVL	automatic vehicle location
AVM	automatic vehicle monitor
B911	basic 911
BCH	Bose-Chaudhuri-Hocquenghem
BOS	backward only smoothing
BP	burst period
BPF	bandpass filter
BPSK	binary phase shift keying
BS	base station
CDMA	code division multiple access
CDVCC	coded digital verification color code
CGSA	cellular geographical service area
CIR	channel impulse response
CMRS	commercial mobile radio service
CQM	channel quality measurement
CSMA/CD	carrier sense multiple access with collision detection
CTIA	Cellular Telecommunications Industry Association
dB	decibels
dBm	decibels relative to 1 mW
dBW	decibels relative to 1 W
DCC	digital color code
DCCH	digital control channel
DFT	discrete Fourier transform
DGPS	differential Global Positioning System
DLL	delay lock loop
DOF	degrees of freedom
DOP	dilution of precision
DQPSK	differential quadrature phase shift keying
DRMS	distance root mean squared
DS0	digital signal level 0
DS1	digital signal level 1
DSO	digital storage oscilloscope

DSP	digital signal processor
DTC	digital traffic channel
DT <sub>x</sub>	discontinuous transmission
E911	enhanced 911
EIA	Electronics Industry Association
ERP	effective radiated power
ESN	electronic serial number
ESPRIT	estimation of signal parameters via rotational invariance techniques
FBS	forward - backward smoothing
FCC	Federal Communications Commission
FDD	frequency division duplex
FDMA	frequency division multiple access
FDTC	forward digital traffic channel
FFT	fast Fourier transform
FIR	finite impulse response
FM	frequency modulation
FOCC	forward control channel
FOS	forward only smoothing
FSDR	full scale dynamic range
FSK	frequency shift keying
GA	genetic algorithm
GHz	giga-Hertz
GPS	Global Positioning System
GSM	Group Special Mobile or Global System for Mobile Communications
HDOP	horizontal dilution of precision
HLR	home location registry
HP	horizontal precision
Hz	Hertz
IF	intermediate frequency
<i>iid</i>	independent identically distributed
IRIS	Impulse Response Identification System
ISI	intersymbol interference
ISM	industrial, scientific, and medical
k	kilo or 10 <sup>3</sup>
kbps	kilobits per second
km	kilometer
LOB	line of bearing
LOS	line of sight
LPF	lowpass filter
LS	listening station
LSB	least significant bit
m	meter
MAC	multiple access control
MAICE	minimum information theoretic criterion estimate
Mbps	mega-bits per second
MDL	minimum descriptor length

<b>MHz</b>	<b>mega Hertz</b>
<b>MIN</b>	<b>Mobile Identification Number</b>
<b>MLSR</b>	<b>maximum length shift register</b>
<b>ms</b>	<b>millisecond</b>
<b>MS</b>	<b>mobile station</b>
<b>MUSIC</b>	<b>multiple signal classifier</b>
<b>MVDR</b>	<b>minimum variance distortionless response</b>
<b>NADC</b>	<b>North American Digital Cellular</b>
<b>NASNA</b>	<b>National Association of State Nine One One Administrators</b>
<b>NENA</b>	<b>National Emergency Number Association</b>
<b>ns</b>	<b>nanosecond</b>
<b>OA&amp;M</b>	<b>operation, administration, and maintenance</b>
<b>PBX</b>	<b>private branch exchange</b>
<b>PCM</b>	<b>pulse code modulation</b>
<b>PCS</b>	<b>Personal Communications Service</b>
<b>PE</b>	<b>principle eigenvector</b>
<b>PETRA</b>	<b>peak tracking algorithm</b>
<b><math>P_{FA}</math></b>	<b>probability of false alarm</b>
<b>PIN</b>	<b>personal identification number</b>
<b>PLL</b>	<b>phase lock loop</b>
<b>PN</b>	<b>pseudo noise</b>
<b>POI</b>	<b>probability of intercept</b>
<b>PSAP</b>	<b>public safety answering point</b>
<b>RCC</b>	<b>radio common carrier</b>
<b>RDTC</b>	<b>reverse digital traffic channel</b>
<b>RECC</b>	<b>reverse control channel</b>
<b>RF</b>	<b>radio frequency</b>
<b>RMS</b>	<b>root mean square</b>
<b>RRC</b>	<b>root raised cosine</b>
<b>RRS</b>	<b>recursive running sum</b>
<b>SA</b>	<b>selective availability</b>
<b>SACCH</b>	<b>slow associated control channel</b>
<b>SAT</b>	<b>supervisory audio tone</b>
<b>SCID</b>	<b>super resolved channel impulse delay</b>
<b>SIR</b>	<b>signal to interference ratio</b>
<b>SNR</b>	<b>signal to noise ratio</b>
<b>SOI</b>	<b>signal of interest</b>
<b>ST</b>	<b>signaling tone</b>
<b>SURP</b>	<b>simulated urban radio propagation</b>
<b>SVD</b>	<b>singular value decomposition</b>
<b>TA</b>	<b>time alignment offset</b>
<b>TAM</b>	<b>Toeplitz approximation method</b>
<b>TDMA</b>	<b>time division multiple access</b>
<b>TDOA</b>	<b>time difference of arrival</b>
<b>TIA</b>	<b>Telecommunications Industry Association</b>
<b>TOA</b>	<b>time of arrival</b>

ULA	uniform linear array
VLR	visitor location registry
W	Watt
WBD	wideband data
WCC	wireline common carrier

## Chapter 1: Introduction

### 1.1 Motivation of CMRS Navigation

Navigation and tracking has increased rapidly in the commercial market during the past decade due to advances in firmware design and software algorithms. A major focus on radio location has been directed towards commercial mobile radio services (CMRS), especially in light of subscribers requiring emergency services. Presently, enhanced 911<sup>1</sup> (E911) is available to most wireline subscribers, where the phone is stationed at a fixed address which permits a Public Safety Answering Point (PSAP) operator to access a street address, name, and telephone number from the wireline service providers' subscriber billing database, allowing the operator to callback the subscriber if the initial call was abruptly terminated. The exception to this service is private branch exchanges (PBXs). However, due to the mobile nature of CMRS the subscriber does not have a street address stored in an accessible database for assisting emergency vehicles to the subscriber's location. Presently, the caller's location is only available verbally and in most emergency situations the caller will be disorientated. Coarse positional information may be derived from the cellular infrastructure by utilizing the geographical location of the serving cell site<sup>2</sup>, although this necessarily does not imply that the wireless subscriber is physically closest to this cell site. Furthermore, the cell site geographical coordinates are not very useful as most cells have radii of 1-2 km in urban environments, with the exception of picocells.

---

<sup>1</sup> Basic 911 (B911) emergency systems establish call routing to a PSAP. The PSAP service provider then has the responsibility of connecting the caller to an appropriate emergency response agency or forwarding the caller to another PSAP for response (i.e. due to geographical and jurisdictional coverage regions). The E911 systems must provide additional features that include selective routing of calls to the appropriate PSAP, display of the calling number, address, and in some cases the primary subscriber's name.

<sup>2</sup> The cell site or base station that has the assigned RF voice or control channel of the wireless 911 caller.

The Federal Communications Commission (FCC) released a notice of proposed Rulemaking concerning E911 emergency calling systems on October 19, 1994 [1]. The FCC document proposed that within five years of the rules being adopted, a wireless 911 caller be located in a three-dimensional environment within a radius of no more than 125 m (410 feet) with probability of 100%. As this accuracy requirement was unreasonable, on February 12, 1996, a technology work group composed of representatives of the Cellular Telecommunications Industry Association (CTIA), the Association of Public-Safety Communications Officials-International (APCO), the National Emergency Number Association (NENA), and the National Association of State Nine One One Administrators (NASNA), recommended an alternative [2]. The recommendation requires a wireless location technology capable of a horizontal accuracy of 125 m distance root mean squared (*DRMS*) within five years of the rulemaking being adopted. The elevation component was not required at this time.

The two-dimensional *DRMS* is defined as the square root of the sum of the  $x$  and  $y$  variances.

$$DRMS = \sqrt{\sigma_x^2 + \sigma_y^2} \quad (1.1)$$

It may be noted that the Global Positioning System (GPS) horizontal dilution of precision (HDOP) is defined in terms of *DRMS*, i.e.,

$$\begin{aligned} HDOP &= \frac{DRMS}{\sigma_p} \\ &= \frac{\sqrt{\sigma_E^2 + \sigma_N^2}}{\sigma_p}. \end{aligned} \quad (1.2)$$

Where,  $\sigma_p$  is the standard deviation of the observed pseudo ranges,  $\sigma_E$  is the standard deviation of one dimensional errors in the East (or  $x$  direction), and  $\sigma_N$  is the standard deviation of one dimensional errors in the North (or  $y$  direction).

The horizontal accuracy of 125 m *DMRS* equates to a 63% radial position error of 125 m, assuming  $\sigma_x = \sigma_y$ , and the error distribution is Gaussian. This *DMRS* criterion will be applied to all 911 calls originated in a service area. Wireless carriers are also required to provide the CMRS subscriber's telephone number (Automatic Number Identification or ANI) to the appropriate PSAP for every wireless 911 call. This includes routing 911 calls from radio handsets with no code identification (i.e. no ANI or CMRS serial number), which complicates matters since the PSAP operator does not have the capability of calling back these handsets.

The FCC has adopted the proposed rulemaking for wireless E911 [3, 4] and the regulatory clock for implementing these features was started October 1, 1996. This implies that the phases outlined in the rulemaking must be completed in the following schedule:

- April 1, 1998**      The first phase of wireless caller location must be routed to the appropriate PSAP. This location information includes the subscriber's ANI for callback purposes and also includes the location of the serving cell site or base station.
- October 1, 2001**    The second phase of wireless caller location replaces the geographical location of the serving cell site with the wireless caller's position (latitude and longitude<sup>3</sup>) with a 125 m *DMRS* accuracy.

Furthermore, it should be noted that these requirements apply only if:

- i) the wireless carrier receives a request for these services from a PSAP that is capable of using this information,
- ii) a cost recovery mechanism for providing these services is in place.

---

<sup>3</sup> It may be noted that the FCC did not specify which geodetic datum should be utilized to determine the wireless subscriber's location.

The demand for wireless E911 has been brought about by the tremendous growth of the cellular industry, approximately 30% per year, and the amount of wireless 911 calls made.

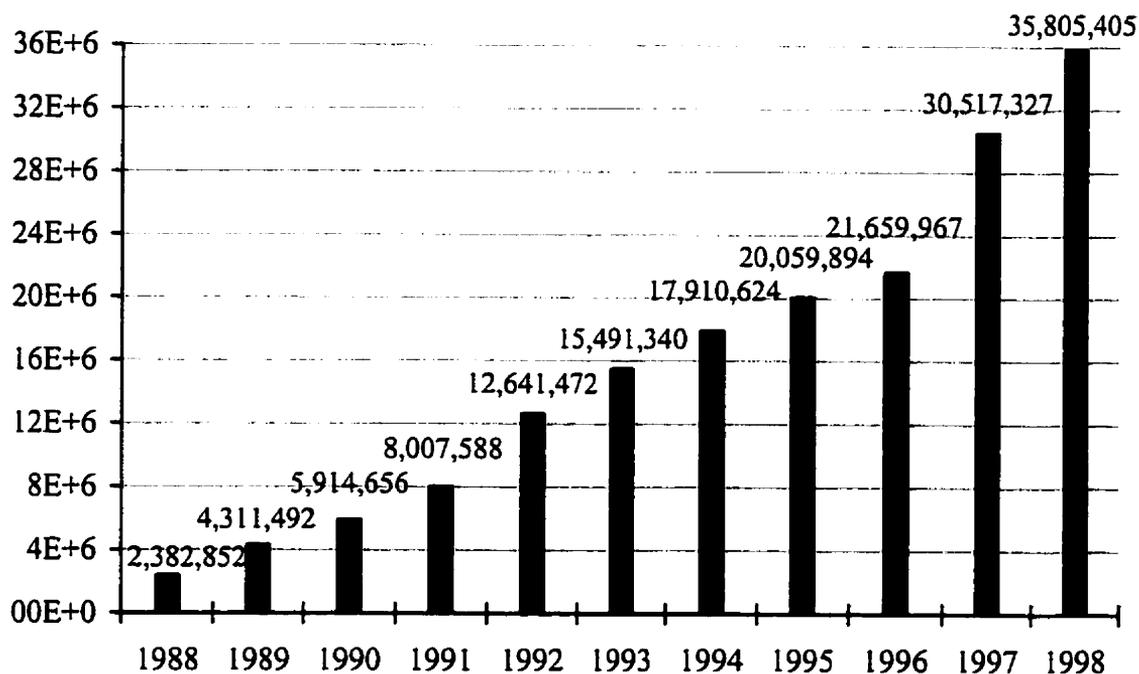


Figure 1.1. Annual cellular 911 calls in the USA [5].

It is estimated that 13% of all 911 calls are made from wireless subscribers. Also many wireless subscribers (approximately 60%) cite safety as the main reason for using a cellular telephone.

Another motivation for CMRS subscriber positioning is wireless telephone fraud. It is estimated that carriers lose more than \$400 million annually due to cellular telephone fraud. This comes from capturing a legitimate subscriber's mobile identification number<sup>4</sup> (MIN); i.e. the subscriber's 10 digit telephone number, and

<sup>4</sup> AMPS, IS-54-B and IS-136 utilize a 10 digit numbering plan in North America, however, the CTIA is in a process of adopting a 15 digit numbering plan similar to that used in Europe.

electronic serial number (ESN) that is transmitted during network access, and copying these to several phones. These clones then have unlimited local and long distance network access until the subscriber's billing account is flagged for having an excessive balance due. By this time the clones will have been reprogrammed with a new MIN and ESN from another unsuspecting subscriber. There are even more sophisticated clones, called tumbling phones, available on the black market for approximately \$1500. These cellular phones are harder to detect because the phone is able to 'tumble' the MIN and ESN rapidly by capturing a legitimate MIN and ESN by being in close proximity to a subscriber when a call is originated. The fraudulent user then accesses the legitimate billing account for a few calls before another MIN and ESN is intercepted, thus, there is no discernible increase in the subscriber's bill. The CTIA is currently developing authentication methodologies that will reduce fraud from off-the-air interception by encrypting the ESN [6], in the mean time some wireless carriers require their subscribers to use a personal identification number (PIN) to obtain network access and service features. However, radio handset service shops keep MIN/ESN records on file for units they have serviced or activated, also wireless carriers retain this data for all their subscribers where unscrupulous employees can easily compromise the subscriber's MIN/ESN.

Since the FCC mandate, several commercial services based on navigation information being available have been proposed, with many more continually being added. These services, mostly revenue generating, will add to the existing services offered by wireless service providers or to the service provider's operational, administrative, and maintenance (OA&M) functionality. These may include or aid the following: location-sensitive billing, electronic yellow pages, fleet management, personnel monitoring, handoff management, radio frequency (RF) planning, dynamic channel allocation. Of course, most of these potential services will require extensive authentication procedures to ensure legal obligations to subscribers for privacy and security since this information can easily be exploited for illegal and immoral purposes.

## **1.2 Existing Navigation Technologies**

During the late 1980's there was a significant rush to obtain patents in the field of mobile radio location in urban/rural environments, which were either based on active or passive principles. A passive system implies that the handset or mobile station (MS) becomes a RF emission point source for several listening stations (LS) that process the MS's signal in either angle-of-arrival (AOA) mode, time-of-arrival (TOA) mode, or time-difference-of-arrival (TDOA) mode. An active system is the reciprocal of a passive system in that the MS now becomes the listening station for several RF emission sources. Examples of active systems are the GPS and automatic vehicle location (AVL) systems operating in the unregulated Industrial, Scientific and Medical (ISM) frequency band of 902-928 MHz. Several individuals further classify the passive and active systems as being network-based (or network-centric) or handset-based technology, respectively. However, this is a common misconception since either approach requires a network for OA&M functionality, as most features are transparent to the end user or subscriber. For example, GPS has a network that constitutes of a constellation of satellites and several terrestrial monitoring stations to provide the required services and features for civilian and military users.

A survey of potential location technologies was compiled by Driscoll and Associates [7], but many of the technologies listed have not produced significant resolution enhancement for narrowband (and wideband) signals. This is primarily due to the location technology being based on conventional radar resolution methodologies, which do not suffer the severe channel distortion that occurs in the mobile radio environment. Even GPS-based systems suffer signal masking effects in the urban environment and differential GPS (DGPS) cannot improve solution accuracy since differential corrections can only account for atmospheric propagation and selective availability (SA). Some of the primary location technologies listed in the Driscoll survey presently have a marketable product and were presented at a recent CTIA workshop [8]

in Washington, DC. These location technologies, handset and network based, were split between AOA and TOA/TDOA processing methods. A few will be briefly described.

KSI Inc. utilizes AOA based technology with suggested accuracies of 125 m in urban environments and up to 1000 m in rural areas with a 90% confidence level. However, the test bed parameters were not released to properly critique the technology and the suggested accuracies. This would include listening station separation and the geometry of the wireless terminal with respect to the listening stations, i.e. dilution of precision (DOP), plus the classification of the mobile radio environment (i.e. the channel delay spread). However, most AOA based products achieve only a  $\pm 3^\circ$  RMS line of bearing on RF sources in a multipath environment under best conditions. This makes monitoring larger cells<sup>5</sup> difficult since horizontal error increases with physical separation.

AccuCom Wireless Services Inc. combines AOA techniques (6 element antenna arrays) along with received signal strength to achieve a suggested 125 m accuracy for two listening stations and 250 m for a single listening station. Again, no details were released on the test bed setup and the parameters that resulted in these accuracies. Other viable technologies presented at the workshop were TOA based. CellTrax performs cross-correlation of either voice channels or signaling channels and uses zero-crossing detection to achieve TOA information, yet, to obtain reasonable positional accuracies the signals are sampled every 50 ns. This results in large data sequences that must be transported to the central processing site via an existing wireline facility at the cell site or a newly installed and dedicated medium (e.g. DS1<sup>6</sup> or fractional DS1 links), which are very expensive.

---

<sup>5</sup> A cell is defined as the geographical area that has telecommunications coverage of the base station equipment located at the cell site.

<sup>6</sup> A DS1 (or T1) facility is a time-division multiplexed pulse code modulated (PCM) link in the North American telephony industry which consists of 24 DS0 channels, each being 64 kbps wide, for a net 1.544 Mbps rate.

The strongest contender was TruePosition™ by The Associated Group Inc., which utilizes wideband receivers (up to 8 adjacent control channels) developed by the Watkins-Johnson Company. The equipment is co-located with cellular base station equipment to process inherent reverse link data messages on the signaling channels. There have been successful field trials in Rochester New York, Philadelphia Pennsylvania, Houston Texas and Baltimore Maryland, but these field trials were conducted on transportable cellular phones, which have a 3W maximum effective radiated power (ERP) and external mounted antennas. Also the environment selected for the *beta* testing is classified as a light urban environment where there are few tall structures and the expected channel delay spread is low, i.e. the confidence level for line-of-sight (LOS) reception is very high. Positioning has yet to be performed on hand-held cellular phones, which have reduced transmit power levels and suffer additional signal-to-noise ratio (SNR) degradation due to antenna orientation and propagation through semi-transparent RF mediums such as glass. The initial estimated deployment cost for TruePosition™ is \$50k per unit, which is expensive for extensive coverage and may cause wireless carriers to deploy minimal equipment to achieve positioning capability in high air-traffic regions only, resulting in inefficient resource utilization.

A final viable product presented at the workshop that deserves an honorable mention is Tandler Cellular, which has integrated a GPS receiver with a cellular phone. What makes Tandler different from numerous other handset-based vendors that utilize GPS is that periodic computed solutions are stored in memory on the integrated unit with the assumption that if GPS signal masking occurs, such as when an individual enters a building, then the last computed solution is used when a 911 call is initiated. The subscriber's position in latitude and longitude and other information are then communicated to the PSAP operator via a voice synthesizer. However, signal masking can occur when the unit is inside a vehicle, so when the wireless subscriber initiates a 911 call an incorrect position may be transferred to the PSAP. Also the accuracies of the computed solution may not be adequate or even available for the mobile subscriber when

an emergency situation arises. This type of integrated unit is geared towards vehicle mounted applications since GPS engines are typically power hungry, where continuous channel tracking and high gain reception are required for the minimal -160 dBW signal availability for the L1 (1575.42 MHz) transmitted signal. Due to the low received signal level, processing gain using 1023 chip length pseudo-noise (PN) sequences are required to extract the signals out of the noise which require continuous arithmetic operations on either digital signal processor (DSP) or application specific integrated circuit (ASIC) designs. Thus, battery life is significantly reduced since this extra consumption is added on top of normal operating requirements of the handset. Although most cellular telephone designs will power off if proper operating voltages cannot be maintained in order to avoid distortion in the RF and digital sections, will the add-on GPS engine be designed with the same “smart monitoring” capability when operating off the same portable cellular battery? If not then there is the possibility of significant errors occurring which the user is unaware of.

Thus, a location technology based on the existing cellular architecture is required, one that will need the least modifications to either the handset or the wireless network. Network-centric systems would be preferable since it would aid the wireless carriers in network OA&M, present services, and future services. A handset-based solution, such as Tandler, are independent of any CMRS air-interface and would be the easiest technology to implement, yet are unable to provide the services allowed by network-centric solutions. Therefore, if the least amount of modifications is required for a network-based solution then existing air-interface signaling (control and voice or traffic channels) must be utilized for AOA positioning, TOA/TDOA positioning, or a suitable hybrid method. This will then require an improved resolution process to obtain the accuracies demanded by the FCC and expected by both the wireless carrier and subscriber<sup>7</sup>.

---

<sup>7</sup> Throughout the remainder of this thesis, subscriber shall imply a CMRS wireless subscriber.

### 1.3 Signal Parameter Resolution

Reception and processing of passband signals; either wideband or narrowband, requires sophisticated techniques in order to mitigate multipath effects. This is especially true when determining LOS arrivals. Conventional time-domain techniques include oversampled correlators with weighted Early-Late decision processes [9-11]; i.e. delay lock loops (DLL). This provides some improvement for determining the LOS arrival, however, it contains an inherent bias if the multipath components have significant amplitude relative to the LOS component. Further improvements are achieved by processing the sampled radio signal in the frequency-domain [12], but there are limitations to the discrete Fourier transform (DFT). Time averaging techniques are then typically applied to minimize measurement and multipath errors but require long observation periods, which are applicable to continuous transmissions and are not useful for burst transmissions that are typical of most CMRS. For example, if we look at the simplistic time-domain correlation method applied to the North American Digital Cellular (NADC) standard [13] which has a symbol duration of approximately  $41.2\mu\text{s}$  and is sampled at a fractional rate,  $R$ , of the symbol duration, then the main correlation time lobe can typically be determined with an accuracy of  $\pm 1/2$  sample or  $\pm 6.2/R$  km. It may be expected that by using narrow correlator technology with high sample rates, like those used in GPS receivers [11], one will resolve the multipath arrivals. However, as the sample rate increases, the correlation lobe lengthens with the additional samples and subsequently the amplitude variation of these samples decrease (i.e. resulting in finite precision effects), making closely spaced arrivals extremely difficult to resolve. Therefore, enhanced resolution techniques are required if processing of existing air-interface messages is desired.

Super-resolution processing has been shown to obtain sub-symbol timing resolution [14-18], which allows TOA processing to be performed with acceptable accuracies in the multipath mobile radio environment. Hence, this approach was adopted in the location methodology of this research. It should be noted that "resolution" is a

subjective entity that varies with each application and individual, and should be clarified. The resolution of the formulated problem model is dependent on the number of degrees of freedom (DOF). Since it is desired to characterize the wireless channel impulse response (CIR), the DOF may include any or all of the following parameters:

- i) number of signal arrivals,
- ii) Doppler frequency or residual frequency,
- iii) signal arrival times,
- iv) signal complex amplitudes,
- v) signal arrival bearing.

The term "signal" is generic, but refers to the true signal and the replicants generated by the specular reflections. One soon realizes that the system solution becomes more complex and nontrivial with each additional DOF, thus, it is desirable to parse the unknown parameters to a computationally acceptable level. Therefore, the primary parameters that are required for wireless subscriber positioning via TOA/TDOA processing are the number of signal arrivals and their associated arrival times.

#### **1.4 Thesis Overview**

This introductory chapter has outlined the motivation of locating wireless terminals and the importance of this application for wireless carriers, especially in light of the recent ruling by the FCC. It is expected that other nations will follow the same legislation once a viable location technology is operating in a commercial application by a wireless service provider.

Chapter 2 provides some foundational history for the use of super-resolution processing in AOA and TOA/TDOA applications [17-21] in order to resolve individual multipath arrivals in the mobile radio environment. These previous applications used the technique of MUSIC and root-MUSIC with success, and also limited accuracy. Two of

these applications were AOA based, where one application [19, 20] used AOA information to locate a wireless terminal while the other application was used to characterize the indoor wireless CIR [21]. The third application [17, 18] is TOA based for wideband signals to obtain sub-chip resolution. Subsequently, this methodology was then applied to determine baselines in an indoor radio environment. The last application was further modified to exploit available information in the algorithmic process in order to improve the TOA estimates, resulting in the development of a LOS candidate selection process in a multiple signal situation and a bias estimation process. This modified version was simulated for wideband signals and then applied to data measurements of an indoor radio environment for baseline determination.

Chapter 3 provides an overview of the North American cellular network, with emphasis on the dual-mode air-network interface which is used for establishing deterministic signals to be used in the TOA estimation process. It may be noted that the present North American cellular architecture is both analog, digital, and multiple code based. However, only the present analog and digital formats will be discussed in the thesis.

Chapter 4 provides two-dimensional location estimates via computer simulations based on the IS-54-B digital mode, for although the system is dual (analog and digital) only the digital mode was initially researched as it was expected that wireless carriers would phase out all analog channels for a fully digital network. The positioning method is based on TOA estimates obtained by the modified super-resolved channel impulse delay (mSCID) method; with bias adjustments, which utilizes the root-MUSIC algorithm. The super-resolved TOA estimates are used in multilateration<sup>8</sup> positioning algorithms.

---

<sup>8</sup> Multilateration is preferred over trilateration as the number of TOA observables is not restricted to be three, although a minimum of three observations is required for two-dimensional positioning.

Chapter 5 will finally conclude the thesis with a brief overview of the material presented. It also proposes some recommendations of super-resolution processing of narrowband CMRS signals, and also discusses potential network integration issues. Relevant future work in the algorithmic process of the SCID and modified SCID methods, and positioning algorithms is also suggested.

## Chapter 2: Eigenvector Projection Estimators

### 2.1 Super-Resolution

The concept of super-resolution was originated by Capon [22] in order to overcome inherent limitations of spectral resolution by classical estimation methods such as the Fourier transform. Spectral estimation of discretely sampled deterministic signals is usually based on processes which utilize the DFT or the fast Fourier transform (FFT). Although these approaches are computationally efficient and produce acceptable results for a large variety of signals, there are inherent limitations of the DFT/FFT. The dominant limitation is its inability to distinguish the spectral responses of multiple signals with minimal angular frequency separation, where the resolution is approximately the reciprocal of the finite time sequence. The window function utilized in the FFT will also manifest itself as leakage in the spectral domain and thus limit the resolution. Even with proper selection of the windowing function, with respect to the signal-of-interest (SOI) and long range/short range leakage minimization, leakage will still occur as the sampled SOI typically is not synchronized with the window function. One may minimize the window synchronization issue with appropriate post-processing, however, the response of the location system should be near real-time as possible, making this method extremely complex.

The usual computational method of FFTs is either in fixed point or floating point precision, with most commercial applications based on fixed point processors. As such, the usual Cooley-Tukey FFT algorithms lose roughly  $k/2$  bits of precision for transforms of vectors of length  $2^k$ . It should be noted that the original elements of the vector to be transformed may have been quantized from values known to greater precision than the  $b$ -bit precision utilized (i.e. to avoid numerical overflow in the finite precision computations). This is usually not a problem unless processing a vector consisting of values that are represented by very few bits.

Computationally, conventional spectral resolution methods such as the spectrogram are very easy to implement since the required calculations involve the FFT of the SOI, and several fast and efficient numerical Fourier transform techniques exist. Yet, as previously mentioned, the windowed observation places a limitation on the estimation accuracy, whether the estimate is based on bearing or arrival time. Therefore, it is desirable to employ large time-bandwidth products such as those used in radar systems, yet this is impossible for CMRS as the available spectrum is limited.

Super-resolution algorithms are able to obtain sub-Rayleigh performance over the classical approaches by utilizing eigenvector manipulation. Although not immune to coherence effects that plague numerous other techniques, it typically offers improved accuracy but at the expense of a higher computational load. The primary subspace-based methods include:

- minimum variance distortionless response (MVDR) [22],
- Toeplitz approximation method (TAM) [23],
- minimum norm [24],
- estimation of signal parameters via rotational invariance techniques (ESPRIT) [25],
- multiple signal classifier (MUSIC) [26].

In addition, several variants of these algorithms exist such as root-MUSIC [27], cyclic-MUSIC [28], etc. In this thesis, only the polynomial variant of the MUSIC algorithm, root-MUSIC is used.

Preliminary applications of super-resolution processing typically focused on unknown frequency estimation [29, 30] and AOA estimation [19, 31-37], yet, some researchers have also applied these algorithms to TOA estimation [14-16]. Despite the results, many researchers tend to shy away from AOA and TOA applications due to significant biases that occur from the coherence of the transmission medium, yet, research is being conducted to minimize these effects. An initial approach was to

decorrelate the data sequence via spatial smoothing [38, 39], which can also be carried over to its temporal counterpart. Newer approaches tend to construct a reduced approximate matrix or a weighted matrix for decomposition in these subspace algorithms [40], in an attempt to better approximate the noiseless case. However, its applicability is limited due to the computational requirements. A brief description of the MUSIC and root-MUSIC algorithms are given below for the sake of continuity. Details are available in [41].

## 2.2 The MUSIC Algorithm

This algorithm was suggested by Schmidt [26] to provide asymptotically unbiased estimates of the number of signal sources, directions of arrival, strengths and cross correlations among the directional waveforms, polarization, and strength of noise/interferers. It is one of the more popular principal eigenvector (PE) algorithms used for high resolution estimation, and is easily adapted for a variety of applications which include frequency estimation, bearing estimation, and time-of-arrival estimation. The problem model of the unknown sources is generally expressed as complex exponentials in diffuse ambient noise, where the sources and noise are assumed to be statistically independent.

Although most applications of the MUSIC algorithm are directed to bearing estimation, the frequency estimation problem will be discussed to illustrate the algorithm procedures and concepts. This is done so that the formulation is performed on a time-based series rather than a joint time/spatial data series. Let  $y[n]$  denote a data sequence which is composed of uniformly sampled  $L$  complex sources (sinusoids) in additive white noise. The duration of the sequence is  $N$  samples and is expressed as

$$y[n] = \sum_{i=1}^L \alpha_i e^{j\omega_i n} + v[n], \quad n = 1, \dots, N,$$

where  $\alpha_i$  and  $\omega_i$  are the unknown (complex) amplitude and angular frequency of the  $i^{\text{th}}$  source, respectively. The complex white noise term  $v[n]$  has zero mean and variance  $\sigma_v^2$ .

In order to improve the performance in a coherent environment, temporal smoothing (or spatial smoothing for bearing applications) is frequently employed. The more common methods include forward-only smoothing (FOS), backward-only smoothing (BOS), and forward-backward smoothing (FBS). The preferred method employed is forward-backward smoothing which forms  $2K$  subsets of  $M$  successive samples from the  $N$  length sequence, where  $K = N - M + 1$ , and it is assumed that  $N \geq M > L$ . This decorrelation method is based on the linear prediction methods of Ulrych *et al.* [42]. The terminology of linear prediction order is dropped, i.e. FOS is preferred over forward linear prediction, since the primary function of the smoothing process is to pre-whiten the data sequence for a prediction method.

Thus,  $M \times 1$  data vectors are formed for the forward process

$$\mathbf{y}_f = [y[i], y[i-1], \dots, y[i-M+1]]^T, \quad i = M, \dots, N, \quad (2.1)$$

and similarly  $M \times 1$  data vectors are obtained for the backward process

$$\mathbf{y}_b = [y[i], y[i+1], \dots, y[i+M-1]]^H, \quad i = 1, \dots, N - M. \quad (2.2)$$

The transpose operator is denoted by  $(\cdot)^T$ , and  $(\cdot)^H$  represents the conjugate transpose operator. The  $M \times M$  covariance matrix of the FBS sequence can be expressed as

$$\begin{aligned} \mathbf{R}_{yy} &= E\{\mathbf{y}\mathbf{y}^H\} \\ &= \sum_{i=1}^L \alpha_i^2 \mathbf{s}_i \mathbf{s}_i^H + \sigma_v^2 \mathbf{I}, \end{aligned} \quad (2.3)$$

where  $E\{\cdot\}$  is the expectation operator, and  $\mathbf{I}$  is the identity matrix. The signal or source vector  $\mathbf{s}_i$ , which corresponds to the frequencies of the unknown sinusoids is defined as

$$\mathbf{s}_i = [1, e^{-j\omega_i}, e^{-j2\omega_i}, \dots, e^{-j(M-1)\omega_i}]^T. \quad (2.4)$$

It would be desirable to extract the signal vectors  $\mathbf{s}_i$  directly from (2.3), but this is not possible. However, the MUSIC algorithm exploits the condition that the  $L$  principal eigenvectors of the covariance matrix span the same subspace as the signal vectors  $\mathbf{s}_1, \mathbf{s}_2, \dots, \mathbf{s}_L$ . Rewriting (2.3) in matrix format, we obtain

$$\mathbf{R}_{yy} = \mathbf{S}\mathbf{P}\mathbf{S}^H + \mathbf{N}, \quad (2.5)$$

where  $\mathbf{N} = E\{\mathbf{v}\mathbf{v}^H\}$  is derived from the receiver channel noise and  $\mathbf{P} = E\{\alpha\alpha^H\}$ . The diagonal elements of  $\mathbf{P}$  represent the ensemble average power levels of the various signal sources. Since the sources are assumed to be uncorrelated then the off-diagonal elements would ideally be zero. The  $M \times L$  frequency (or steering) matrix is defined by

$$\mathbf{S} = \begin{bmatrix} 1 & 1 & \dots & 1 \\ e^{-j\omega_1} & e^{-j\omega_2} & \dots & e^{-j\omega_L} \\ \vdots & \vdots & & \vdots \\ e^{-j(M-1)\omega_1} & e^{-j(M-1)\omega_2} & \dots & e^{-j(M-1)\omega_L} \end{bmatrix}. \quad (2.6)$$

In accordance with the usual eigenvalue problem statements, one obtains

$$|\mathbf{R}_{yy} - \lambda_i \mathbf{I}| = 0 \text{ and } \mathbf{R}_{yy} \mathbf{v}_i = \lambda_i \mathbf{v}_i,$$

where  $\lambda_i$  are the eigenvalues of  $\mathbf{R}_{yy}$ , and  $\mathbf{v}_i$  are the associated eigenvectors. These eigenvectors are orthogonal to one another and make up the columns of the matrix  $\mathbf{V}$ , given below:

$$\begin{aligned} \mathbf{R}_{yy} &= \mathbf{V}\Sigma\mathbf{V}^H \\ &= \sum_{i=1}^{2K} \lambda_i \mathbf{v}_i \mathbf{v}_i^H. \end{aligned} \quad (2.7)$$

The term principal eigenvector implies those eigenvectors which correspond to the unique eigenvalues generated by the distribution (i.e. signal plus noise), while the non-principal eigenvectors correspond to the small eigenvalues generated by the receiver channel noise. Under ideal conditions the non-principal eigenvalues are identical and

equal to the receiver channel noise power level, i.e.  $\sigma_v^2 = \lambda_v$ . Thus, one may rewrite (2.7) to emphasize the PE, obtaining

$$\mathbf{R}_{yy} = \sum_{i=1}^L (\lambda_i - \lambda_v) \mathbf{v}_i \mathbf{v}_i^H + \lambda_v \mathbf{I}. \quad (2.8)$$

We may now write

$$\mathbf{SPS}^H \mathbf{v}_i = 0 \quad \forall i = L+1, \dots, M, \quad (2.9)$$

since  $\mathbf{v}_i \perp \mathbf{v}_j$  for  $i \neq j$ .

Thus, the signal vector may be obtained by finding those angular frequencies that are orthogonal to the noise subspace, rather than a direct estimate on the signal subspace in the Euclidean sense. In practice, the ensemble covariance matrix  $\mathbf{R}_{yy}$  is unknown, but can be estimated from the available data, i.e.,

$$\begin{aligned} \hat{\mathbf{R}}_{yy} &= \frac{1}{2K} \mathbf{A}^H \mathbf{A} \\ &= \mathbf{V} \mathbf{\Sigma} \mathbf{V}^H. \end{aligned} \quad (2.10)$$

Where the  $2K \times M$  data matrix  $\mathbf{A}$  constitutes the vectors  $\mathbf{y}_{f_M}, \dots, \mathbf{y}_{f_N}$ , and  $\mathbf{y}_{b_1}, \dots, \mathbf{y}_{b_{N-M}}$  of the FBS method, i.e.,

$$\mathbf{A}^H = \begin{bmatrix} \mathbf{A}_f & \mathbf{A}_b \end{bmatrix}. \quad (2.11)$$

$$\mathbf{A}_f^T = \begin{bmatrix} y[M] & y[M-1] & \dots & y[1] \\ y[M+1] & y[M] & \dots & y[2] \\ \vdots & \vdots & & \vdots \\ y[N] & y[N-1] & \dots & y[N-M] \end{bmatrix}$$

$$\mathbf{A}_b^T = \begin{bmatrix} y^*[1] & y^*[2] & \dots & y^*[M] \\ y^*[2] & y^*[3] & \dots & y^*[M+1] \\ \vdots & \vdots & & \vdots \\ y^*[N-M] & y^*[N-M+2] & \dots & y^*[N] \end{bmatrix}.$$

Here we denote the complex conjugation operator by  $(\cdot)^*$ , and the preferable subset vector length (or prediction order) of the FBS method is given by  $M = \lceil \frac{3}{4} N \rceil$ .

The MUSIC null spectra is then given by

$$\begin{aligned} \hat{S}_{MUSIC}(\omega) &= \frac{1}{D(\omega)} \\ &= \frac{1}{\mathbf{s}^H(\omega) \mathbf{V}_N \mathbf{V}_N^H \mathbf{s}(\omega)} \\ &= \frac{1}{\sum_{i=L+1}^M |\mathbf{s}^H \mathbf{v}_i|^2}, \end{aligned} \quad (2.12)$$

where the frequency (or source) vector  $\mathbf{s}(\omega)$  is now expressed as

$$\mathbf{s}(\omega) = [1, e^{-j\omega}, e^{-j2\omega}, \dots, e^{-j(M-1)\omega}]^T.$$

Without knowledge of the number of sources,  $L$ , it is preferable to over fit the model, which leads to an over-determined system of equations. Thus, the reduced rank method is required, and works well as long as the SNR does not fall below a threshold, i.e. as the noise increases then so do the singular values corresponding to the noise subspace. Therefore, either the wrong source singular value is truncated or a non-source singular value is kept. When this occurs there is a catastrophic decrease in performance rather than a gradual decrease. The singular value decomposition of a given distribution has the same property as that of the Fourier series of a continuous signal, that in principle, an infinite number of terms is required to represent the distribution exactly. However, from previous experiences with series representations, a desirable level of accuracy can be achieved with only a finite number of terms. A main advantage of performing such a reduction is that if the desired signal is embedded in a noisy environment, only the first few terms of the decomposition are necessary to represent the signal. The noise level will then be significantly reduced since the noise is typically spread out over all terms of the decomposition. Of course the question arises as to how

many terms are sufficient to represent the signal. The singular values or  $\sigma$ 's, obtained from the decomposition contain a unique classification of the distribution and hence can be readily used since one is just comparing numbers, typically by using ratios of the singular values such as the Euclidean distance. Different methods to estimate the number of sources,  $L$ , also exist, where the more popular methods include Akaike's minimum information theoretic criterion estimate (MAICE) [43, 44] and Rissanen's minimum descriptor length (MDL) [45].

To illustrate the above derivation, the following example is presented. The data samples are generated by the expression

$$y(n) = e^{j(2\pi f_1 n + \phi_1)} + e^{j(2\pi f_2 n + \phi_2)} + v(n), \quad n = 0, 1, \dots, N-1,$$

where  $f_1 = 0.52$  Hz,  $f_2 = 0.50$  Hz,  $\phi_1 = \pi/4$ ,  $\phi_2 = 0$ , and  $v(n)$  are independent complex Gaussian noise samples with variance  $2\sigma^2$  for both the real and imaginary components. The SNR is then defined as  $10 \log_{10} \left( \frac{1}{2\sigma^2} \right)$ , the sample rate is assumed to be 1 Hz, and the sequence length is 25 samples ( $N = 25$ , hence  $M = 18$ ). Thus, after performing an extensive search of  $\omega$ , the following is obtained, where the peak components correspond to 0.50 Hz and 0.52 Hz.

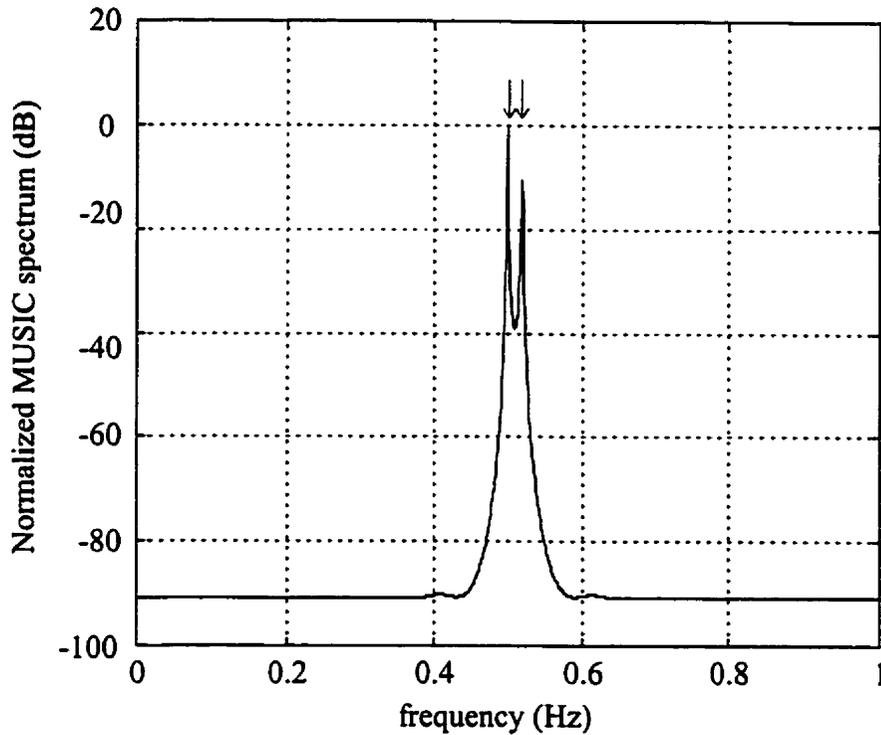


Figure 2.1. Frequency estimator for the two source example at 20 dB SNR, where the MUSIC Null spectra has been normalized.

It is clearly evident that this algorithm produces very large peaks in  $\hat{S}_{MUSIC}(\omega)$  for good covariance matrix estimates, because of the aforementioned orthogonality of the noise subspace to the source vector space.

Since the sample covariance matrix  $\hat{\mathbf{R}}_{yy}$  and the Hankel structured data matrix  $\mathbf{A}$  are related; as shown below, it is preferable to perform the singular value decomposition (SVD) directly on the data matrix  $\mathbf{A}$ , where the conditioning of  $\mathbf{A}$  provides slightly improved performance over the covariance matrix. Given that the complex matrix  $\mathbf{A} \in \mathbf{M}_{m,n}$  can be written as  $\mathbf{A} = \mathbf{U}\mathbf{\Sigma}\mathbf{V}^H$ , we may obtain the following:

$$\begin{aligned}
\mathbf{A}\mathbf{A}^H &= (\mathbf{U}\Sigma\mathbf{V}^H)(\mathbf{U}\Sigma\mathbf{V}^H)^H \\
&= \mathbf{U}\Sigma\mathbf{V}^H\mathbf{V}\Sigma^T\mathbf{U}^H \\
&= \mathbf{U}\Sigma\mathbf{I}\Sigma^T\mathbf{U}^H \\
&= \mathbf{U}\Sigma\Sigma^T\mathbf{U}^H,
\end{aligned} \tag{2.13}$$

and similarly

$$\mathbf{A}^H\mathbf{A} = \mathbf{V}\Sigma^T\Sigma\mathbf{V}^H. \tag{2.14}$$

Here  $\mathbf{U} \in \mathbf{M}_m$  and  $\mathbf{V} \in \mathbf{M}_n$  are unitary matrices, and  $\Sigma$  is a diagonal matrix with non-negative entries.

Thus,

$$\Sigma = [\sigma_{ij}] \in \mathbf{M}_{m,n}, \text{ where } \sigma_{ij} = 0 \forall i \neq j, \tag{2.15}$$

and

$$\sigma_{11} \geq \sigma_{22} \geq \dots \geq \sigma_{kk} > \sigma_{k+1,k+1} = \dots = \sigma_{qq} = 0, \tag{2.16}$$

where  $q = \min\{m, n\}$ , and  $\{\sigma_{ii}\} \equiv \{\sigma_i\}$  are the non-negative square roots (singular values) of the eigenvalues of  $\mathbf{R} = \mathbf{A}^H\mathbf{A}$ .

Hence, the MUSIC algorithm can be summarized as follows:

- i) Generate the data matrix  $\mathbf{A}$  from the subset vectors  $\mathbf{y}_{f_i}$  and  $\mathbf{y}_{b_i}$ . Recall that several decorrelation methods exist for obtaining the subset vectors beside the FBS method.
- ii) Compute the SVD of either the sample covariance matrix or the data matrix.
- iii) Estimate the modes or number of sources,  $\hat{L}$ , if it is unknown. This is usually done by determining a gap in the ordered eigenvalues obtained from the previous step. Several methods of mode determination exist and are described in [43-45].
- iv) Determine the angular frequencies from the MUSIC null spectrum,  $\hat{S}_{MUSIC}(\omega)$ .

The above formulation can readily be adapted for high resolution beamforming with a uniform linear array (ULA), although a ULA is not mandatory for the MUSIC algorithm. The time samples are replaced with spatial samples, where the substitution  $\omega_i = 2\pi \frac{d}{\lambda} \sin \theta_i$  is made. The array inter-element spacing is represented by  $d$ ,  $\lambda$  is the common RF wavelength, and  $\theta_i$  is the direction of the  $i^{\text{th}}$  source.

It may be noted that the sample covariance matrix can be augmented by another technique, where several signal snapshots or observation periods are jointly processed. Thus, the data matrix becomes

$$\mathbf{A}^H = \begin{bmatrix} y[N,1] & \cdots & y[N,P] & y^*[1,1] & \cdots & y^*[1,P] \\ y[N-1,1] & \cdots & y[N-1,P] & y^*[2,1] & \cdots & y^*[2,P] \\ \vdots & & \vdots & \vdots & & \vdots \\ y[2,1] & \cdots & y[2,P] & y^*[N-1,1] & \cdots & y^*[N-1,P] \\ y[1,1] & \cdots & y[1,P] & y^*[N,1] & \cdots & y^*[N,P] \end{bmatrix}, \quad (2.17)$$

$$= [\mathbf{A}_f \ \mathbf{A}_b]$$

where the matrix  $\mathbf{A}^H$  contain  $N \times 1$  column vectors of the sampled signal taken at distinct observation intervals  $1, 2, \dots, P$ . This technique is frequently used in radar applications since the signal is repeated at a known repetition rate, where the period is sufficiently short such that the channel characteristics do not change significantly. This augmentation process is limited in digital CMRS processing applications since the mobile radio channel can change drastically over consecutive TDMA frames, and will also be affected by the timing tolerance of the MS. For example, the IS-54-B standard allows a maximum timing variation of  $\pm 1/8$  symbol period between consecutive TDMA frames. Thus, this potential jitter can reduce the resolution of the multiple snapshot process.

One may note that the frequency matrix utilized in the MUSIC algorithm, i.e. (2.6), is a Vandermonde matrix,  $\mathbf{S} \in M_n(F)$ , which is of the form



The roots of  $D(z)$  correspond to the sources, that is,  $D(z)|_{z \in \{e^{j\omega_1}, \dots, e^{j\omega_L}\}} = 0$  such that  $D(0) \neq 0$ . Hence, evaluating the null spectrum  $\hat{S}_{MUSIC}(\omega)$  is equivalent to evaluating the reciprocal of the polynomial  $D(z)$  in the complex plane, where the peaks of  $\hat{S}_{MUSIC}(\omega)$  correspond to the roots of  $D(z)$  lying close to or on the unit circle.

The root-MUSIC algorithm proceeds exactly as the MUSIC algorithm to the determination of the null spectrum, which is replaced by the polynomial  $D(z)$ .

Therefore, the signal vector  $\mathbf{s} = \mathbf{s}(\omega) = [1, e^{-j\omega}, e^{-j2\omega}, \dots, e^{-j(M-1)\omega}]^T$  of the unknown frequency estimation process becomes  $\mathbf{s} = [1, z^1, z^2, \dots, z^{M-1}]^T$ .

$$\therefore D(z) = \sum_{i=-(M-1)}^{M-1} d_i z^i \quad (2.19)$$

One may observe that  $D(z)$  is a conjugate symmetric polynomial, i.e.  $d_{-i} = d_i^*$ . Hence, because of this relation, the roots of  $D(z)$  occur in reciprocal conjugate pairs. If  $z_1$  is a zero of  $D(z)$ , then  $\frac{1}{z_1^*}$  is also a zero. Thus, the zeros of the polynomial constitute paired roots of the source and non-source components, where the roots reside on both sides of the unit circle.

Using the same two source example for frequency estimation in section 2.2, where  $f_1 = 0.52$  Hz,  $f_2 = 0.50$  Hz,  $\phi_1 = \pi/4$ ,  $\phi_2 = 0$ , and  $v(n)$  are independent complex Gaussian noise samples, Figures 2.2 - 2.3 are obtained from root-MUSIC when FBS is employed.

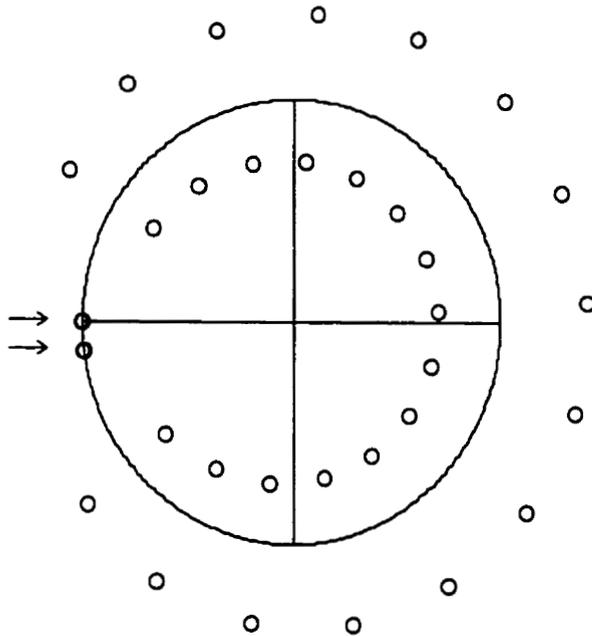


Figure 2.2. Polynomial zeros for the two source frequency estimation example at 20 dB SNR.

It may also be observed that  $D(z)$  exhibits orthogonal polynomial behavior, being that the polynomial zeros are nearly symmetrically distributed about the complex unit disk, with an approximate angular separation of  $\Delta\theta = \frac{2\pi}{m}$ , where  $2m$  is the exact degree of  $D(z)$ .

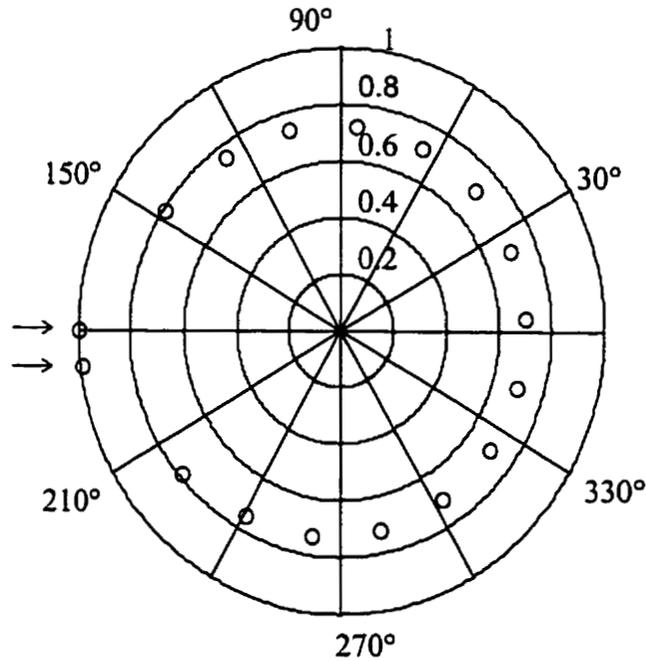


Figure 2.3. Polynomial zeros for the two source frequency estimation example at 20 dB SNR, reciprocal zeros (roots outside the unit circle) are not illustrated.

The root pairs  $\{z_i, (z_i^*)^{-1}\}$ ,  $i = 1, \dots, \tilde{L}$ , which correspond to the sources should lie on the unit circle, where the angular frequency of the source is determined from the phase angle of the polynomial root. Therefore, the root phases that correspond to the two sources in Fig. 2.3 are  $\arg\{z_{\tilde{L}}\}_{\tilde{L}=1,2} \cong \{0.99999\pi, 1.04030\pi\}$ , which then becomes

$$f_{\tilde{L}} = \frac{\arg\{z_{\tilde{L}}\}}{2\pi T_s} \cong \{0.49999, 0.52015\} \text{ Hz, where } T_s \text{ denotes the sample period.}$$

The root locations may become perturbed by reduced SNR, measurement errors, coherency effects, and finite precision effects, such that they will depart from the unit circle. However, a benefit of this polynomial method is that any radial perturbations of the signal root pairs will not affect the angular frequency estimate, which might otherwise reduce the peaks of the MUSIC null spectrum, as shown in Fig. 2.4.

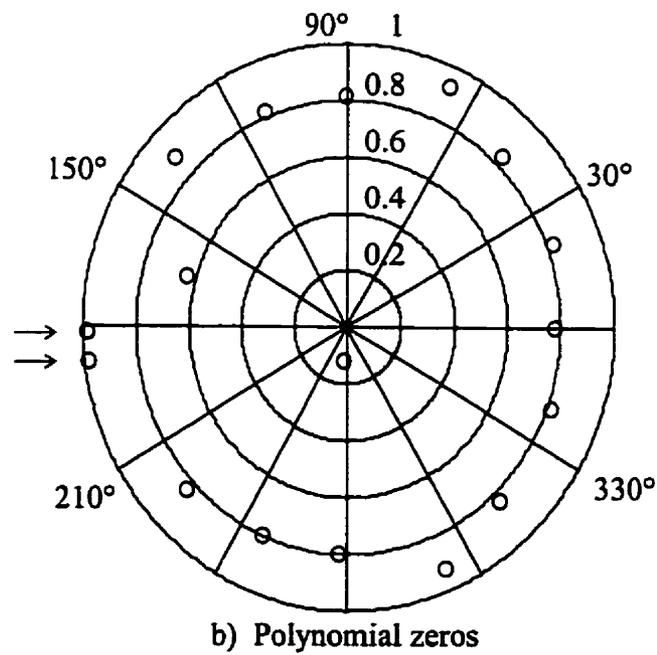
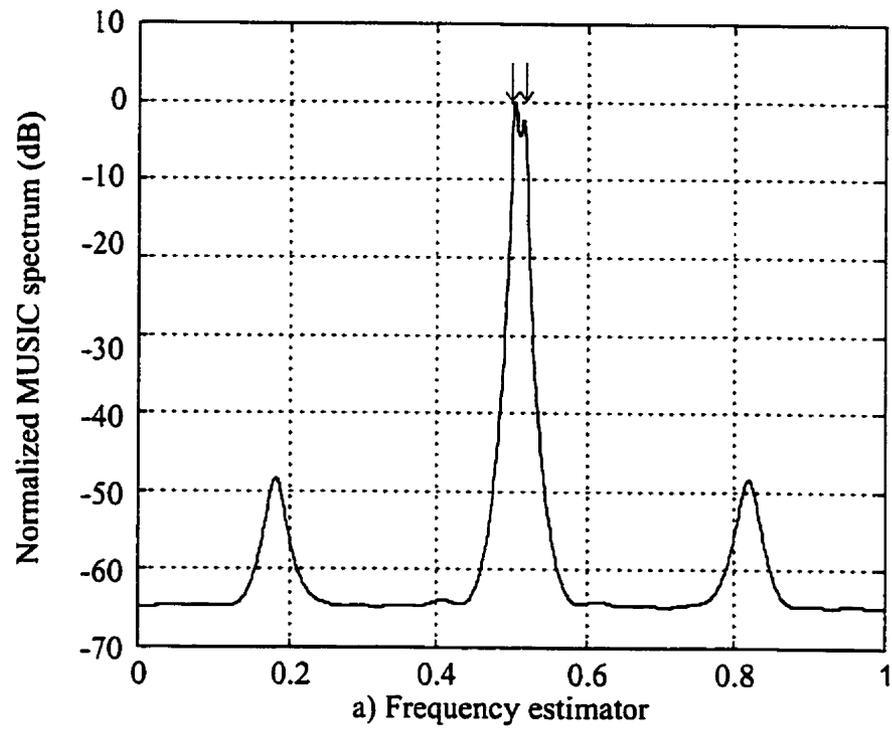


Figure 2.4. Frequency estimator and polynomial zeros for the two source example at 15 dB SNR, reciprocal zeros are not illustrated.

Thus, the radii of the roots play a central role in the selection process. Not only must the root angle have sufficient accuracy to represent the source, but the root radius must be adequate to distinguish it from the non-source or extraneous roots. This selection criteria will be relaxed later in the TOA estimation model as the signal root pair selection will be confined to an angular sector of the unit circle. This approach will aid the selection process in low SNR conditions, and will be discussed in section 2.9.2.

Therefore, the root-MUSIC algorithm can be summarized as follows:

- i) Generate the data matrix  $\mathbf{A}$  from the subset vectors  $\mathbf{y}_{f_i}$  and  $\mathbf{y}_{b_i}$ . Recall that several decorrelation methods exist for obtaining the subset vectors besides the FBS method.
- ii) Compute the SVD of either the sample covariance matrix or the data matrix.
- iii) Estimate the modes or number of sources,  $\hat{L}$ , if it is unknown.
- iv) Construct and root the polynomial  $D(z)$ . An efficient method of determining the polynomial coefficients is to utilize  $d_i = \text{tr}_i(\mathbf{V}_N \mathbf{V}_N^*)$  for  $i = -(M-1), \dots, 0, \dots, M-1$ . Where  $\text{tr}_i(\cdot)$  denotes the trace of the  $i^{\text{th}}$  diagonal of the matrix,  $i = 0$  corresponds to the main diagonal,  $i > 0$  is above the main diagonal and  $i < 0$  is below the main diagonal.
- v) Select the  $\tilde{L}$  signal roots and determine its associated angular frequency.

For the noiseless case, and assuming that the sources are sufficiently separated such that they are easily discernible, the number of modes can be perfectly estimated via the obtained singular value (or eigenvalue) distribution, i.e.  $\hat{L} = L$ . Under these same assumptions, the polynomial root pairs associated with the sources should also be identifiable, thus,  $\tilde{L} = L$ . However, under realistic measurement conditions, the estimated modes and determined source root pairs may not be exact, i.e.  $\hat{L} \neq \tilde{L} \neq L$ .

It may be of interest to the reader that AOA estimation via the root-MUSIC algorithm requires the use of a ULA, however, Friedlander has developed an interpolating approach such that any arbitrary array geometry may be used [46].

#### **2.4 AOA Super-Resolution Processing of Radio Frequency Signals**

Several researchers [31-37] have applied super-resolution processing on AOA information using large antenna arrays, however, another researcher, Klukas [19, 20], used an approach that was unique in that a smaller antenna array was utilized. Rather than using large cumbersome antenna arrays that would only be applicable for vehicle mounted applications, a simple two antenna array was used to produce a larger virtual array by sampling the antenna array while in motion (either linear or non-linear motion). Typical AOA direction finding applications are restricted to a small customer base due to the size of the arrays required and the cost of necessary equipment, as the antenna arrays must be phase calibrated when the signal wavefronts are combined for digital conversion and processing. This has made the concept of a large temporal antenna a very attractive one. However, the super-resolution process still suffers from coherency effects, not all of which comes from multipath but also from the mutual coupling of the antenna array elements. Pasala and Friel [47] took the mutual coupling effects into consideration before processing the AOA information with super-resolution and were able to reduce bias errors in the spectral estimates, but a large computational burden was created for the decoupling process.

Now Klukas' primary motivation for positioning mobile radios using AOA information was for air-traffic management, i.e. aiding pages and handoffs. The application of subscriber location for emergency services, anti-criminal services, or navigation services were not considered important at that time. Simulations were run using the modified Simulated Urban Radio Propagation (SURP) program by Fattouche *et al.* [48]. Hashemi [49] developed the original propagation program (SURP) based on

extensive mobile radio channel measurements and modeled the associated slow-fading characteristics, yet modifications were required to account for fast-fading characteristics. In his research work, Klukas made the assumptions that the multipath components of the outdoor radio channel were clustered, as was observed in the outdoor radio environment [49, 50] and also in the indoor radio environment [51]. These reflected and scattered signals are clustered due to the localized environment of the RF emission source. In his work, only an active location method was accounted for, i.e. positioning was performed at the subscriber's side using multiple RF signals from base stations within the receiver's RF reception range.

Subsequently, in his research Klukas developed the Peak Tracking Algorithm (PETRA) process, which utilizes the MUSIC algorithm for determining the signal arrivals. MUSIC with temporal (forward-backward) smoothing was employed in order to obtain some degree of decorrelation in the highly coherent narrowband environment. The PETRA process would evaluate the MUSIC null spectrum for varying numbers of signal arrivals or sources. Typically, a fixed eigenvalue threshold process is used to estimate the number of sources, which may not always be accurate. Thus, it was decided to evaluate several spectral estimates by varying the number of estimated cluster arrivals, i.e.  $\hat{L} = 1, \hat{L} = 2, \dots$ . To minimize the computational load, the number of arriving clusters was upper bounded to three. Thus, PETRA evaluated the MUSIC spectra for a single cluster arrival, then two, and finally three. An immediate disadvantage of this approach is that the computational burden is increased threefold as the MUSIC spectra is evaluated for the three mode variants.

It was clear from Klukas' results [19, 20] that the AOA determination method has two common difficulties associated with the MUSIC algorithm:

- i) correct mode estimation,
- ii) determining the resultant LOS source from the candidate set.

The results achieved by the computer simulations indicate the process would be well suited for microcell applications, however, further improvements would be necessary to adopt the same process in larger cells.

Klukas had proposed that AOA processing at the base stations be investigated, i.e. a passive system, which may be ideal since many smart antenna structures are currently being implemented for improved signal reception in next generation wireless systems. However, the deployment of the new smart antenna architectures may be lengthy as simpler mature networks are firmly entrenched and profitable for existing subscriber densities. Furthermore, AOA performance degradation may occur due to the limited transmit power levels of the MS.

Presently, AOA-based location technology has been shown to be viable but these technologies all suffer the same limitations in that the position accuracy degrades with increased RF reception coverage even though the bearing accuracy will be upper bounded. Typical *RMS* bearing errors have been shown to be low, and in fact most commercial products have bearing errors that range from  $\pm 3^\circ$  to  $\pm 5^\circ$  *RMS* in a multipath environment. If the following assumptions can be made:

- i) the angular error is low,
- ii) the traversed arc length due to the angular error is much smaller than the baseline.

One may then approximate the traversed arc with a perpendicular length of  $2h$ , where  $h = d \tan \theta_{rms}$  (see Fig. 2.5).

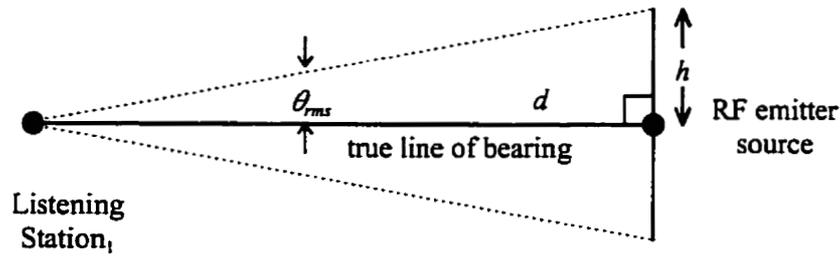


Figure 2.5. Line of bearing accuracy.

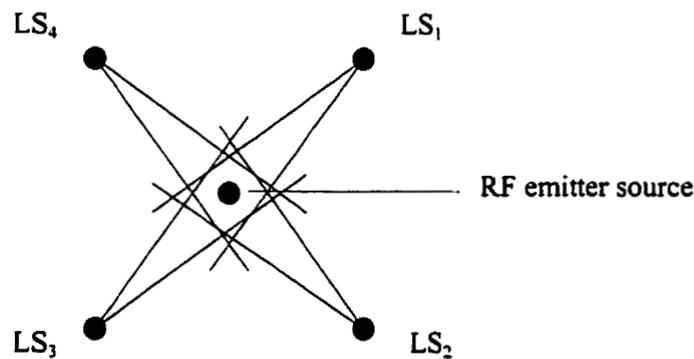


Figure 2.6. Line of bearing accuracy on two-dimensional positioning.

Subsequently, if one envisions an RF emitter located at the centroid of say four equally distributed listening stations with each having the same line of bearing (LOB) accuracy (Fig. 2.6), then the emitter position can exist anywhere in an approximate square area of  $4h^2$  or  $4d^2 \tan^2 \theta_{rms}$ . Thus, it is clearly illustrated that the position error is dependent on the coverage area. Therefore this method becomes impractical for CMRS applications as it is desirable to use the existing cellular network architecture or as much of that architecture that is possible. It may be noted that the coverage area may be reduced by installing pseudo base stations, primarily to achieve multiple signal reception in troublesome RF coverage regions.

Another researcher, Tholl [21] examined the UHF indoor radio channel for small scale spatial variations of the multipath components. These components were then divided into sub-components which arrive in nearly the same time interval but at unique

bearings. These modeled channel characterizations were based upon 12,000 CIR measurements in two separate buildings (AGT Tower and NovAtel Communications Ltd., both located in Calgary, Alberta, Canada). In this CIR modeling, it was found that a high correlation existed in small displacements of a portable antenna while the combination of multipath rays from adjacent reflectors/scatterers remained similar. In the method of analysis, spatial signal processing was used to determine the bearing and estimate the complex magnitude of the sub-components within a resolvable multipath component (i.e. cluster). The MUSIC algorithm, with forward-only smoothing, was employed and briefly compared with the minimum-norm algorithm. Subsequently in this form of analysis, it was found that MUSIC produced a smoother noise floor than the minimum-norm method, which tended to produce spurious peaks. This was expected since rank reduction was not performed, which significantly reduces the represented noise level.

## 2.5 TOA Super-Resolution Processing of Radio Frequency Signals

The TOA estimation model of the MUSIC algorithm was previously proposed by Bruckstein *et al.* [14], and others [15-18]. The usual model entails the multipath reception of a signal of known shape  $c(t)$ . Assuming that the multipath channel consists of  $L$  discrete paths, each with a unique time delay, then the impulse response of the multipath channel can be expressed as

$$h(t) = \sum_{i=1}^L \alpha_i \delta(t - \tau_i), \quad (2.20)$$

where  $\alpha_i$  and  $\tau_i$  are the complex amplitude and lag for the  $i^{\text{th}}$  transmission path, respectively. The multipath channel output then becomes

$$\begin{aligned} y(t) &= h(t) * c(t) + n(t) \\ &= \sum_{i=1}^L \alpha_i c(t - \tau_i) + n(t) \end{aligned} \quad (2.21)$$

where  $*$  denotes convolution, and  $n(t)$  is additive white gaussian noise with zero mean and variance  $\sigma_n^2$ . The complex exponentials representing the unknown frequencies in the MUSIC frequency estimation problem are now replaced by the known complex signal  $c(t)$ . Thus, the source vector, i.e. (2.4), becomes

$$\mathbf{s}_i = \left[ c(t_1 - \tau_i), c(t_2 - \tau_i), \dots, c(t_M - \tau_i) \right]^T, \quad (2.22)$$

which is then used in (2.12) to obtain the lag estimates.

Dumont *et al.* [17, 18] also achieved sub-chip timing resolution of TOA estimates for wideband CIRs by employing the root-MUSIC algorithm. However, the model was first taken to the frequency domain to deconvolve system filter responses, which may influence the delay estimates. Thus, the time delay estimation problem is transformed to estimating complex exponentials in colored Gaussian noise, where the source frequencies are inversely proportional to the unknown multipath lags. This processing method shall be referred to as the super-resolution channel impulse delay (SCID) method.

## 2.6 The SCID Method

This frequency domain approach is well suited for the MUSIC algorithm and its polynomial variant, in that the time estimator model is naturally expressed as exponentials in noise. Although the noise becomes colored by the receiver filters, the smoothing process is able to minimize these effects, such that the noise component appears white over the processing bandwidth.

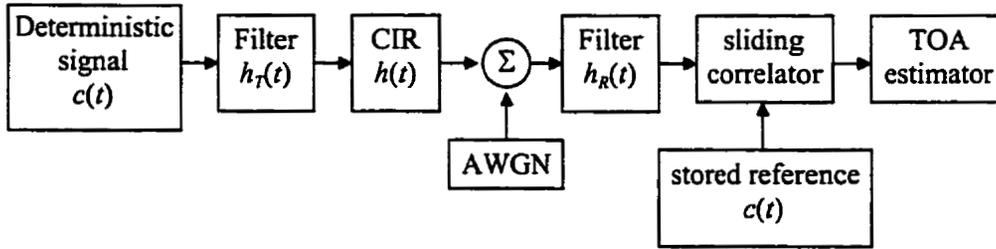


Figure 2.7. Baseband equivalent model of the TOA estimator.

The above figure illustrates the lowpass equivalent scheme for estimating the TOA for a passband transmission system, where the transmit and receive filters may encompass pulse shaping for minimizing intersymbol interference (ISI) and lowpass filtering to suppress out-of-band emissions. The sliding correlator depicted above may also be equivalently replaced by a matched filter. The output of the transmitter block becomes

$$x(t) = h_r(t) * c(t), \quad (2.23)$$

where  $h_r(t)$  denotes the overall transmit filter impulse response. Thus, the multipath channel output is obtained similarly by convolving  $x(t)$  with (2.20), resulting in the time domain expression

$$y(t) = \sum_{i=1}^L \alpha_i x(t - \tau_i) + n(t), \quad (2.24)$$

or equivalently in the frequency domain as

$$Y(f) = \sum_{i=1}^L \alpha_i e^{-j2\pi f\tau_i} X(f) + N(f). \quad (2.25)$$

The prefilter output of the receiver yields

$$R(f) = \sum_{i=1}^L \alpha_i e^{-j2\pi f\tau_i} X(f) H_R(f) + \beta_1(f), \quad (2.26)$$

where  $H_R(f)$  is the Fourier transform of  $h_r(t)$ , and  $\beta_1(f)$  is nonstationary uncorrelated random noise of power spectral density  $S_{\beta_1}(f) = \frac{\sigma_n^2}{2} |H_R(f)|^2$ . Hence, the correlator output becomes

$$P(f) = \sum_{i=1}^L \alpha_i e^{-j2\pi f \tau_i} X(f) H_T(f) H_R(f) C^*(f) + \beta_2(f), \quad (2.27)$$

where the colored noise term of (2.26) has undergone further spectral shaping by  $C^*(f)$ .

The TOA estimator then performs a deconvolution of the combined filter responses in the frequency domain via the DFT (or FFT). Rather than using a large data vector of the correlated output sequence for the DFT deconvolution, Dumont limits the data vector to contain the correlation lobe and finite adjacent regions on either side. Thus, the discrete sampled sequence is centered about the determined main correlation time lobe, which provides some isolation from discernible signal arrivals, allowing the process to focus on and estimate the closer spaced arrivals. This approach provides a two stage classification of the channel time delays:

- i) An initial coarse absolute TOA,  $\tau_c$ , is obtained which corresponds to the midpoint of the finite time domain vector. Where the data sequence will be transformed to the frequency domain for further processing.
- ii) A super-resolved relative time adjustment,  $\Delta\tau_i$ , is obtained at the output of the SCID process.

The finite sampled sequence is also adjusted for DC (i.e. 0 Hz) offsets, which are estimated from a region preceding the compressed code. This is done to minimize discontinuities that may occur at 0 Hz when the sequence is mapped to the frequency domain, where the relative TOA estimates may be perturbed by the smoothing process.

Therefore, the deconvolution process obtains

$$\begin{aligned} \hat{H}(f) &= \frac{P(f)}{H_T(f) H_R(f) C(f) C^*(f)} \\ &= \sum_{i=1}^L \alpha_i e^{-j2\pi f \tau_i} + \beta(f), \end{aligned} \quad (2.28)$$

where the noise term remains uncorrelated and nonstationary, i.e.,

$$\beta(f) = \frac{N(f)}{H_T(f)C(f)}. \quad (2.29)$$

One now takes  $N$  frequency domain sample points of the deconvolved sequence centered about 0 Hz, i.e.  $|f| \leq f_{dp} = \frac{N-1}{2} f_s$ , where the sampling frequency is given by  $f_s$ . This data sequence is to be used in the root-MUSIC algorithm, where the FBS data matrix  $\mathbf{A}$  is constructed, i.e. (2.11). The bandlimited sequence ensures that the poorly estimated passband edges are not used, which occur from the rolloff and stopband regions of the associated filter responses used in the deconvolution.

It may be noted that if  $H_T(f)C(f)$  may be considered constant over the utilized bandwidth, then it would only be necessary to deconvolve  $H_R(f)C^*(f)$ . One would still have to account for the filter lags of  $h_T(t)$  and  $c(t)$ . Furthermore, the noise component  $\beta(f)$  would be white over the finite bandwidth.

$$\therefore \hat{H}(f) = \frac{P(f)}{H_T(f)H_R(f)C(f)C^*(f)}, \quad |f| \leq f_{dp}$$

The source root pairs  $\{z_i, (z_i^*)^{-1}\}$ ,  $i = 1, \dots, \tilde{L}$ , and their associated phase angles  $\theta_i$  are then converted to the relative time estimates  $\Delta\tau_i$ . Dumont determined the potential candidate set of source roots by selecting those polynomial zeros that lie in the annulus  $r_o \leq |z| \leq 1$ , where  $r_o = 0.9$ . Thus, the super-resolved phase angles of the candidate set  $\theta_i = \arg\{z_i\}$  are substituted into

$$\Delta \tau_i = \frac{1}{f_s} \left[ \frac{-\theta_i}{2\pi/N_{FFT}} - T_w \right], \quad (2.30)$$

where an  $N_{FFT}$ -point FFT (or DFT) is used in the deconvolution process, and  $T_w$  is the sample lag of the  $N$  length time-based data vector.

The high resolution absolute time estimates; excluding filter lags (both hardware and software based), become

$$\hat{\tau}_i = \tau_c + \Delta \tau_i, \quad i = 1, \dots, \tilde{L}, \quad (2.31)$$

where the LOS component is dictated by  $\min\{\Delta \tau_i\}_{i=1, \dots, \tilde{L}}$ . In the event that the candidate set remains empty, i.e.  $\tilde{L} = 0$ , then the resultant absolute time estimate defaults to the coarse resolution estimate  $\tau_c$ .

To illustrate the process described above, Fig. 2.8 shows the results obtained for a two source example, where the LOS and non-LOS components are of equal amplitude and phase, i.e.  $\alpha_i = e^{j0}$ . The associated path lags are given by  $\tau_1 = 1000 \text{ ns}$  and  $\tau_2 = 1050 \text{ ns}$ . The reference code utilized is a maximum length shift register (MLSR) sequence with period  $P = 2^7 - 1$ , and generator polynomial  $g(p) = p^7 + p^6 + 1$  (initialized at zero). The sequence is assumed to have a symbol period of  $T_{symbol} = 100 \text{ ns}$ , and is uniformly sampled at a fractional rate of  $T_{symbol}/4$ . Matched finite impulse response (FIR) lowpass filters (LPF) are used at both the transmitter and receiver, where the LPF coefficients are derived from a  $N = 25$  sample Hamming weight of an ideal brick wall filter response, i.e.,

$$h[n] = \frac{1}{2} \text{sinc} \left( 2 \frac{f_c}{f_s} (n - k) \right) \left( 0.54 + 0.46 \cos \left( 2\pi \frac{n - k}{N - 1} \right) \right), \quad n = 1, \dots, N.$$

Where  $f_c$  and  $f_s$  denote the cutoff frequency (12 MHz) and sample frequency (40 MHz), respectively. Also,  $\text{sinc}(\cdot) = \frac{\sin \pi(\cdot)}{\pi(\cdot)}$ , and  $k = \frac{N-1}{2} + 1$  since  $N$  is odd. Thus, the LPF has an approximate passband of  $f_{-3dB} \cong 10$  MHz, and a 64 - point FFT was utilized.

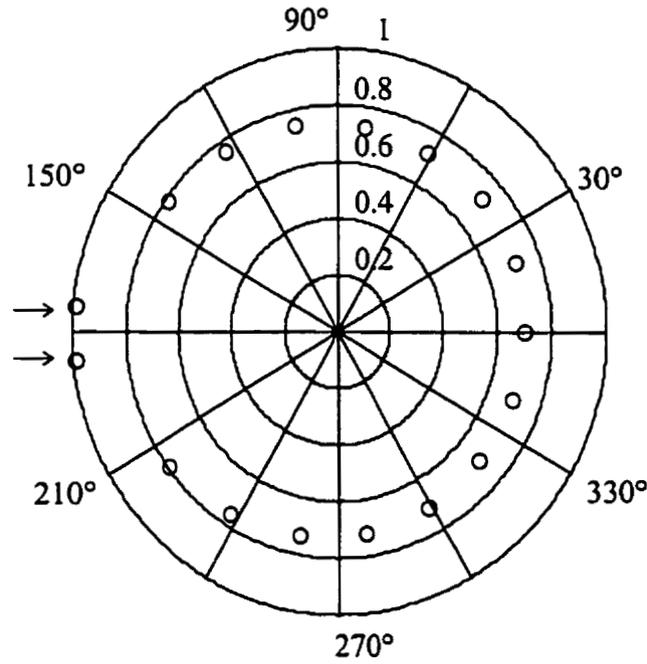


Figure 2.8. Polynomial zeros of TOA estimator for two sources at 20 dB SNR.

The dimensionality of data vectors are  $N = 25$  and  $M = 18$ , the coarse time estimate is  $\tau_c = 1025$  ns, and the window (rectangular) lag is  $T_w = 32$  samples. The root phases corresponding to the two sources in Fig. 2.8 are  $\arg\{z_{\bar{z}}\}_{\bar{z}=1,2} \cong \{0.97084\pi, 1.03235\pi\}$ .

Thus, the relative time adjustments are given by

$$\Delta \tau_i|_{i=1,2} = \frac{1}{40 \text{ MHz}} \left[ \frac{-\arg\{z_L\}}{2\pi/64} - 32 \right] \cong \{-25.88, 23.33\} \text{ ns}, \text{ obtaining the final source}$$

estimates of  $\hat{\tau}_1 \cong \tau_c - 25.88 \text{ ns} = 999.12 \text{ ns}$  and  $\hat{\tau}_2 \cong \tau_c + 23.33 \text{ ns} = 1048.33 \text{ ns}$ .

Thus, the SCID method may be summarized as follows:

- i) Obtain the cross-correlation of the received sequence and the code  $c(t)$  either by time or frequency based techniques.
- ii) Determine the main correlation lobe corresponding to the LOS component. The lobe is then time referenced; i.e.  $\tau_c$ , truncated, and adjusted for the estimated DC offset component.
- iii) Perform the FFT or DFT deconvolution of the truncated correlation lobe, and bandlimit the deconvolved sequence to  $|f| \leq f_{dp}$ .
- iv) Utilize the root-MUSIC algorithm on the FBS data matrix  $\mathbf{A}$ , which is constructed from the deconvolved and bandlimited sequence.
- v) Convert the phase angle of the source roots to the relative time adjustments, and determine the high resolution TOA estimate for the LOS component.

It may be noted that the phase of the transformed signal  $P(f)$  may be retained and the magnitude set to unity as an alternative to evaluating (2.28), i.e.,

$$P(f) = |P(f)| e^{j\Theta(f)} \quad (2.32)$$

$$\therefore \hat{H}(f) \approx e^{j\Theta(f)}$$

where  $|P(f)|$  is the zero phase (magnitude only) component and  $\Theta(f)$  is the continuous phase component. Although numerical division is still required to obtain the data vector to be utilized in the root-MUSIC algorithm, a direct normalization approach can be used.

This approach does not require memory storage of the filter complex responses, but is of limited use as the TOA estimates degrade rapidly as the number of sources increase.

## 2.7 SCID Architecture Considerations

### 2.7.1 Code Compression

The cross-correlation of the received deterministic signal and the stored replicant can be performed either in the time or frequency domain. The frequency domain correlation has the benefit of utilizing the processing gain of a  $N_{FFT}$ -point FFT (or DFT), especially if the vector length (zero padded or not) is significantly greater than the sample duration of the compressed code, i.e.  $p_o(t) = \frac{1}{T} \int c(\tau)c^*(\tau-t)d\tau$ . This is extremely beneficial in low SNR observations which occur in remote interceptions. However, depending on firmware architecture and computation latency in performing the frequency domain correlation, it may be necessary to restrict the signal interception method to a time domain approach. Thus, the frequency domain correlation may then be applied in a pseudo post-process fashion, as illustrated below.

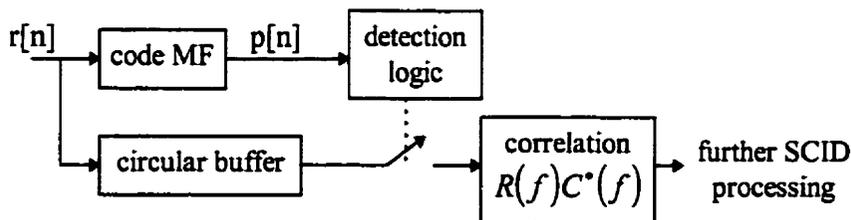


Figure 2.9. Block diagram of a real-time SOI interceptor.

It should be noted that this approach will have a performance level that is lower bounded by the received SNR and signal-to-interference ratio (SIR) since the detection is solely dictated by the time domain interception method.

### 2.7.2 Sample Reduced Correlation Sequence

Once the cross correlation vector is obtained; either by frequency or time based methods, it is then truncated to a limited region about the determined main correlation time lobe. Prior to truncation, the resultant correlation sequence will exhibit periodic components (i.e. cyclostationarity) that occur due to the sample rate being higher than the Nyquist rate, the transmission channel being dispersive, and from the utilized code (data patterns) and its modulation format. This periodicity may manifest itself as leakage when the correlation vector is transformed to the frequency domain, where it will further propagate through the SCID process as the frequency domain mapped data vector undergoes smoothing to generate the data matrix  $A$ . For example, assume that the obtained cross-correlation vector contains a dominant time lobe and two additional lobes of significant magnitude, i.e. a precursor and postcursor. These sidelobes are then symmetrically distributed about the main lobe as illustrated in the figure below.

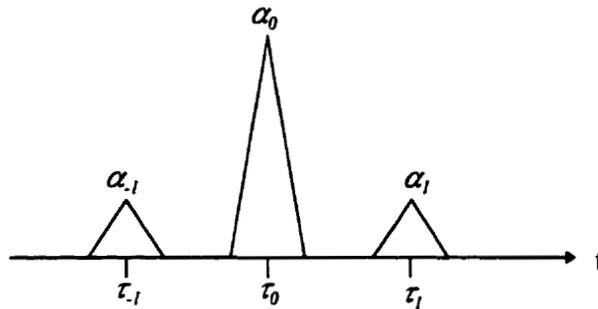


Figure 2.10. Illustration of harmonic properties of cross-correlation sequences.

If all three lobes have an equivalent base of  $2T$ , then by mapping the data vector to the frequency domain we obtain

$$P(f) = \alpha_{-1} T \text{sinc}^2(fT) e^{-j\omega\tau_{-1}} + \alpha_0 T \text{sinc}^2(fT) e^{-j\omega\tau_0} + \alpha_1 T \text{sinc}^2(fT) e^{-j\omega\tau_1}.$$

These self generated time sidelobes will then behave as multipath, adding bias and variance to the locations of the signal root pairs. As mentioned, this effect is minimized in the processing method by either properly truncating the correlation vector or using an

appropriate weight function (i.e. a non-rectangular window). Thus, the narrowed observation containing the main time lobe achieves additional noise quieting effects as the self generated sidelobes are not processed. Hence, the operator must determine an appropriate vector length and weight function (rectangular or otherwise) for satisfactory performance, where a balance must be achieved between the time-bandwidth product (i.e. vector length) and the time resolution of the compressed code,  $p_o(t)$ , in the multipath channel.

### 2.7.3 Mode Estimation

As no prior information exists regarding the rank of matrix  $\mathbf{A}$ , it must then be estimated from the SVD components. This reduced rank approximation then allows the extension of the SNR threshold for the over-determined model. Dumont utilized a fixed threshold based on the spectral radius of the sample covariance matrix to estimate the number of singular vectors (or eigenvectors) that correspond to the signal-plus-noise subspace, which adds little computational overhead compared to those methods that perform exhaustive searches over the whole singular value (or eigenvalue) subset [43-45].

**Definition:** The set of all  $\lambda \in \mathbf{C}$  that are eigenvalues of  $\mathbf{B} \in \mathbf{M}_n$  is called the spectrum of  $\mathbf{B}$  and is denoted by  $\sigma(\mathbf{B})$ . The spectral radius of  $\mathbf{B}$  is the nonnegative real number  $\rho(\mathbf{B}) = \max\{|\lambda|: \lambda \in \sigma(\mathbf{B})\}$ , i.e. it is the absolute value of a point in the spectrum  $\sigma(\mathbf{B})$  that is maximum distance from the origin.

Dumont had used a scale factor of  $10^2$ ; which may have been experimentally determined, to obtain the following eigenvalue comparison threshold, i.e.,

$$\lambda_{threshold} = \frac{1}{100} \rho(\mathbf{A}^H \mathbf{A}). \quad (2.33)$$

It appears that Dumont selected this scale factor since the size of the data matrix  $\mathbf{A} \in \mathbf{M}_{m,n}$  used was  $\{m,n\} = \{14,19\}$ , and  $10 < \min\{m,n\} = 14$ . Since the SVD is a nonlinear operator, a direct threshold value which is proportional to the spectral radius has merit. However, since the matrix was smoothed, the preferable scale factor should have been chosen based on the number of generated subsets, i.e.  $2(N - M + 1)$ , used to construct  $\mathbf{A}$ . One may note that if an arbitrary scale factor is chosen then the reduced representation will not adequately model the sources, and hence, either too many singular vectors (or eigenvectors) are kept or too many are discarded. It should also be noted that the mode estimator described above, the MAICE [43, 44] and the MDL [45] methods, all tend to overestimate the number of sources in low SNR conditions since the non-principal singular values (or eigenvalues) tend to increase in magnitude, resulting in a drastic degradation in estimator performance. Similarly, the same mode estimators tend to underestimate the sources in a coherent environment.

#### 2.7.4 Candidate Roots

For the TOA estimation model, there is no definitive method to determine which polynomial root pair corresponds to the first signal arrival. In fact this remains a problem in most applications of the root-MUSIC algorithm, whether the estimator is based on angle or time arrivals. Selecting the signal root from the root-MUSIC algorithm is usually based on a magnitude criterion, where the polynomial roots that reside closest to or on the complex unit disk are designated as the source roots and the subsequent root that has the largest magnitude (upper bound to unity) is designated as the first arrival in TOA applications. However, this approach of root selection is not entirely accurate, especially for the cases of disjoint or directly attenuated channel impulse responses. Determining the source roots is further complicated in low SNR conditions where the root pairs associated with the desired source will not only deviate in phase but also in magnitude. Hence, a static annulus,  $r_o \leq |z| \leq 1$ , for determining the candidate roots is inappropriate.

If we examine the two source TOA example from section 2.6, with the exception that the first arrival is now 20 dB below the multipath component, the following is obtained.

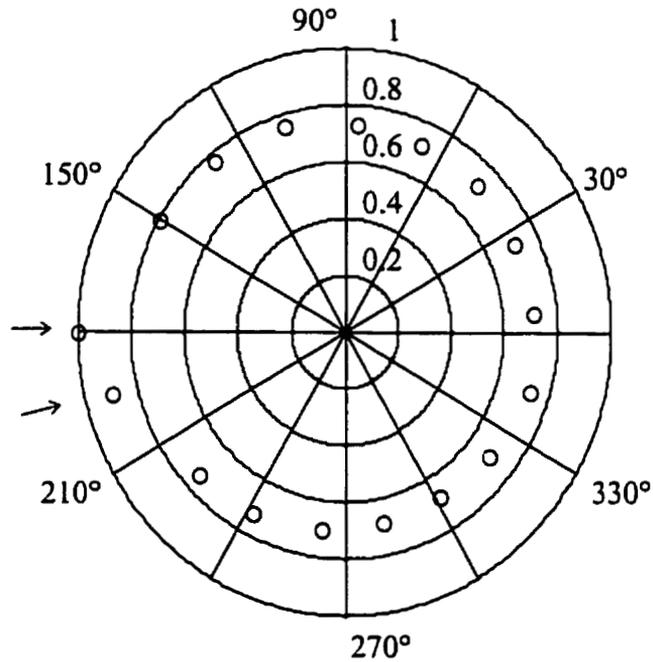


Figure 2.11. Polynomial zeros of TOA estimator for two sources at 20 dB SNR, where  $\alpha_1/\alpha_2 = 0.1$  (i.e. -20 dB). The dimensionality of data vectors are  $N = 25$ ,  $M = 18$ .

Here, both sources exist, yet only the root associated with the secondary arrival is selected as a candidate since its magnitude lies within the static annulus, i.e.  $0.9 \leq |z| \leq 1$ .

If both source roots were selected, the time estimates would be  $\hat{\tau}_1 \cong \tau_c - 64.68 \text{ ns}$  and  $\hat{\tau}_2 \cong \tau_c - 1.53 \text{ ns}$ , where  $\tau_c = 1050 \text{ ns}$ .

One may derive an ad hoc dynamic annulus from the initial inclusion region of the polynomial coefficients, i.e. a disk centered at the origin with a radius that contains all zeros of a polynomial  $p(z)$ . Given the following polynomial of degree  $m$

$$p(z) = d_0 + d_1z + d_2z^2 + \dots + d_{m-1}z^{m-1} + d_mz^m, \quad (2.34)$$

let  $\lambda_1, \dots, \lambda_m$  be positive numbers such that

$$\sum \lambda_i \leq 1. \quad (2.35)$$

The inclusion radius,  $R$ , for  $p(z)$  is then given by the expression

$$R = \max_{1 \leq k \leq m} \lambda_k^{-1/k} \left| \frac{d_{m-k}}{d_m} \right|^{1/k}, \quad (2.36)$$

such that

$$|z_i| \leq R, \quad i = 1, \dots, m. \quad (2.37)$$

Thus, if one lets  $\lambda_k = \left(\frac{1}{2}\right)^k$ , then the inclusion radius becomes

$$R = \max_{1 \leq k \leq m} 2 \left| \frac{d_{m-k}}{d_m} \right|^{1/k}.$$

If one recalls, the polynomial  $D(z)$  is reciprocal conjugate symmetric, i.e.  $d_{-i} = d_i^*$ ,

hence, we can surmise that  $r_1 \leq |z| \leq r_2$ . Where  $r_1 = \max_{1 \leq k \leq m} \frac{1}{2} \left| \frac{d_{m-k}}{d_m} \right|^{-1/k}$  and  $r_2 = R$ .

The lower bound of the dynamic annulus is then determined by

$$r_o = 1 - (\min |z| - r_1). \quad (2.38)$$

Thus, applying (2.38) to the above ill-solved example (Fig. 2.11), the following results are obtained.

Table 2.1: Magnitude of Polynomial Coefficients

$i$	$ d_{-i}  =  d^*_i $	$i$	$ d_{-i}  =  d^*_i $
17	0.0964	8	0.2851
16	0.1343	7	0.5380
15	0.1935	6	0.7010
14	0.1648	5	0.9938
13	0.1914	4	1.1824
12	0.1610	3	1.3622
11	0.1719	2	1.5921
10	0.0549	1	1.7355
9	0.1556	0	16.000

Using Table 2.1,  $r_1 = \frac{1}{2} \left| \frac{d_{10}}{d_{17}} \right|^{-1/7} \cong 0.5418$  and  $r_2 = 2 \left| \frac{d_{15}}{d_{17}} \right|^{1/2} \cong 2.8327$ , hence,

$r_o \cong 1 - (0.6883 - r_1) = 0.8535$ . The source radii are  $|z_1| \cong 0.8936$ ,  $|z_2| \cong 0.9937$ , and the next largest root radius is  $|z| \cong 0.7914$ . Hence, both source roots lie within the designated annulus.

Another aspect of the polynomial zeros is the method by which they are obtained. The usual polynomial rooting algorithms reduce the complexity of the operations by performing deflation, thus, as each root  $z_i$  is found the polynomial is factored to produce a polynomial of lower degree, e.g.  $p(z) = (z - z_i)p_i(z)$ . One soon realizes that since the factored polynomials are generated from the finite precision determination of the roots, accumulative errors will occur in the determination of the subsequent coefficients of the consecutive deflated polynomials. A typical approach for minimizing the cumulative errors is done by examining the derivatives of the initial roots (i.e. critical points). However, other approaches that do not require the determination of the critical points exist, i.e. those that employ Weierstrass' corrections. This topic is extensively covered in [52] for the interested reader. Therefore, from the preceding discussion, it may be

preferred to utilize the source roots that reside outside the unit circle as the numerical accuracy of the determined phase angle may be slightly improved.

### 2.7.5 DC Estimation

One may recall that once  $\hat{H}(f)$  is obtained, it is necessary to bandlimit the data vector to a region where  $\hat{H}(f)|_{|f| \leq f_p}$  is a smooth function, which removes the poorly estimated passband edges. A similar discontinuity will also occur at 0 Hz due to DC coupled effects in the signal conversion process, where these values can significantly affect the MUSIC null spectra and its corresponding orthogonal polynomial (especially when smoothing is employed). One should therefore exercise caution with the DC estimation method employed. The 0 Hz adjustment on the time-domain sequence may not be adequate when the sequence is mapped to the frequency domain so one may alternatively perform the 0 Hz adjustment on the frequency domain data.

## 2.8 The Modified SCID Method

The modified process for the SCID method (mSCID) follows the foundation outlined by the SCID process, with minor differences in the mode estimator and the 0 Hz offset estimation. The mSCID process, instead, uses a new candidate root selection method, and a new bias estimation process. A greater emphasis of the process is also placed on minimizing the spectral discontinuities of  $\hat{H}(f)$ , and subsequently improving the conditioning of the data matrix, i.e.  $\kappa(\mathbf{A})$ , prior to decomposition. This conditioning is achieved by further reducing the utilized bandwidth and performing the 0 Hz adjustment in the frequency domain rather than in the time domain. The DC offset is easily interpolated from the adjacent low frequency values of the transformed compressed code (i.e. prior to deconvolution), a process which is more accurate than an average of  $k$  complex samples prior to the correlation time lobe.

Thus, the modified SCID method may be summarized as follows:

- i) Obtain the cross-correlation of the received sequence and the code  $c(t)$  either by time or frequency based techniques.
- ii) Determine the main correlation lobe corresponding to the LOS component. This lobe is then time referenced and truncated.
- iii) Perform the FFT or DFT of the sequence, and adjust for the estimated 0 Hz offset. The sequence is then deconvolved and bandlimited to  $|f| \leq f_{dp}$ .
- iv) Utilize the root-MUSIC algorithm on the FBS data matrix  $\mathbf{A}$ , which is constructed from the deconvolved and bandlimited sequence.
- v) Estimate the bias of the phase angles corresponding to the sources, and adjust them accordingly. Convert the adjusted phase angles of the source roots to the relative time adjustments, and determine the high resolution TOA estimate for the LOS component.

## 2.9 Modified SCID Architecture Considerations

Once the correlation sequence has been transformed to the frequency domain, the hardware/firmware system effects are removed. These effects include the frequency response of the filters utilized on the transmit and receive portions, the correlation response, and the window function. Since the transmitter will represent a transportable phone in the end application, the exact filters to be utilized are left to the discretion of the handset manufacturer. Although the frequency response of the pulse shaping filters are known, the manufacturer is usually allowed some flexibility in implementation, as long as a squared error function is bound within a prescribed tolerance. Therefore, one may have to further restrict the bandwidth of the deconvolved sequence, or modify the reference filter response used in the deconvolution such that the attenuation rolloff occurs at a lower rate (i.e. to minimize large discontinuities at the band edges).

### 2.9.1 Mode Estimation

The mode estimator utilized in the MUSIC and root-MUSIC algorithms follows the same approach taken by Dumont due to its computational ease over the MAICE and MDL methods, with the exception that the scale factor used was based on the smoothing process used to generate the data matrix. Thus, the new comparison singular value threshold for estimating the modes is given by

$$\begin{aligned}\hat{\sigma}_{threshold} &= \sqrt{\frac{1}{2(N-M+1)} \rho(\mathbf{A}^H \mathbf{A})} \\ &= \sqrt{\frac{1}{2(N-M+1)}} \sigma(\mathbf{A})\end{aligned}\quad (2.39)$$

where FBS is employed. Therefore,  $\sigma_i \geq \hat{\sigma}_{threshold}, \forall i = 1, \dots, 2(N - M + 1)$  corresponds to the principal or signal-plus-noise singular values. As previously mentioned, this method will have difficulties in low SNR conditions and coherent environments. The effects of coherence becomes very noticeable on the mode and TOA estimates when the time separation between the sources become smaller than the approximate lower bound of

$$\Delta t = \frac{N}{(M-1)f_s}, \quad (2.40)$$

where  $N$  and  $M = \lceil \frac{3}{4}N \rceil$  are the vector sizes used in the data matrix.

Hence, if the application is required to resolve small source separations due to the channel characteristics, then the operator must appropriately balance the parameters  $\{N, M, f_s\}$  for the expected CIR.

### 2.9.2 Candidate Roots

Once the mode order,  $\hat{L}$ , is estimated from the singular value distribution, the polynomial  $D(z)$  is then generated and its roots obtained. The operator must then determine the  $\tilde{L}$  source root pairs, where the usual selection method encompasses the candidate set consisting of root radii lying within a defined annulus on the unit circle.

However, *a priori* information exists on the expected source root locations, which can be exploited to aid the selection process. Since the data vector contains the centered correlation lobe, which is then mapped to the frequency domain, the polynomial source root selection can be confined to a phase corridor on the complex plane. The windowed correlation time lobe thus corresponds to extraneous noise root pairs equally distributed about the complex plane, with the root pair(s) associated with the clustered arrival lying in a finite region that corresponds to the lag of the windowed time lobe, i.e.  $T_w$ .

If we re-examine the TOA estimation example used for Fig. 2.11, with the exception that the window lag is accounted for in the deconvolution process then Fig. 2.12 is obtained.

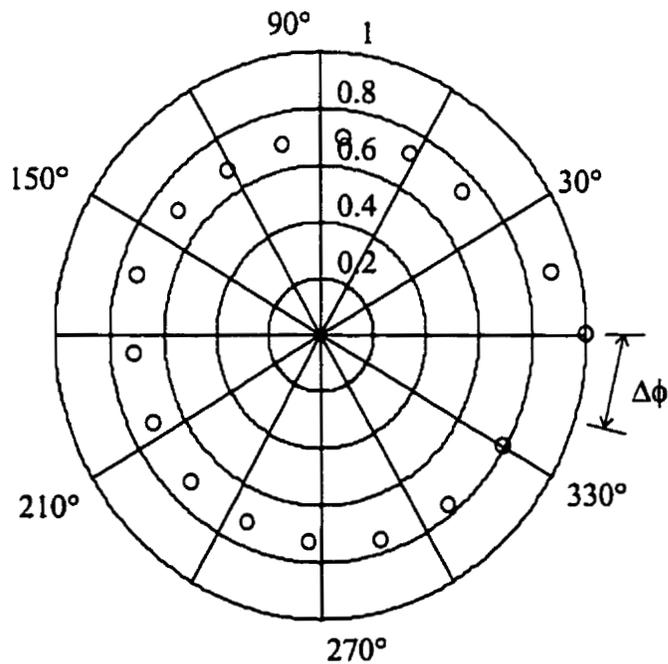


Figure 2.12. Polynomial zeros of TOA estimator for two sources at 20 dB SNR, where  $\alpha_1/\alpha_2 = 0.1$  (i.e. -20 dB). The dimensionality of data vectors are  $N = 25$ ,  $M = 18$ .

Thus, the expected source root(s) would lie on the complex unit disk with an approximate phase corresponding to  $T_w$ , where  $T_w = 0$  if the window lag was accounted for in the deconvolution process. Therefore, the polynomial root pair selection can be localized to a  $-2\pi f_s T_w \pm \Delta\phi$  phase corridor. The value of  $\Delta\phi$  should be of an appropriate margin to allow for small phase perturbations, yet not large enough that the extraneous roots are mistakenly selected as source roots, i.e.,

$$\Delta\phi \leq 2\pi \frac{k}{N_{FFT}} < \frac{2\pi}{m}, \quad (2.41)$$

where  $k$  is typically the symbol period in samples, and  $2m$  is the exact degree of  $D(z)$ . Of course, one may always utilize a joint selection method which combines the phase corridor process and a magnitude criteria for selecting the candidate roots.

Since the root pairs are reciprocal, there is the option of either selecting those signal roots that reside within the unit circle, i.e.  $|z_i| \leq 1$ , or the corresponding reciprocal roots that lie outside the unit circle. As previously mentioned, it may be desirable to select those root candidates that lie outside the complex unit disk due to the polynomial rooting algorithm being implemented in finite precision.

### 2.9.3 Bias Estimation

The approximation of a matrix by another of lower rank solves the very important linear prediction problem. If one lets  $\mathbf{A}$  denote a rank  $p$  matrix and considers the error between it and a rank  $r$  approximation to it, then one obtains

$$e^2 = \text{tr}(\mathbf{A} - \mathbf{A}_r)^H (\mathbf{A} - \mathbf{A}_r). \quad (2.42)$$

This error term is called the Frobenius norm of  $\mathbf{A} - \mathbf{A}_r$ , which is the sum of squares of all the elements. Thus, the reduced approximate becomes  $\mathbf{A}_r = \mathbf{U}\Sigma_r\mathbf{V}^H$ , where  $\Sigma_r = \text{diag}[\lambda_1, \dots, \lambda_r, 0, \dots, 0]$ .

$$\begin{aligned} \therefore e^2 &= \text{tr } \mathbf{V}(\boldsymbol{\Sigma} - \boldsymbol{\Sigma}_r) \mathbf{U}^H \mathbf{U}(\boldsymbol{\Sigma} - \boldsymbol{\Sigma}_r) \mathbf{V}^H \\ &= \sum_{i=r+1}^p \lambda_i \end{aligned} \quad (2.43)$$

The main problem lies in determining what  $r$  is, i.e. mode estimate, and hence the reduced rank of  $\mathbf{A}$ . But that decision directly affects each of the subspaces of  $\mathbf{A}$ , and hence their calculation via the  $\text{SVD}(\mathbf{A})$ . Thus, since the MUSIC algorithm relies on the projection of the noise-free source vector onto the noise subspace, one can assume that biases that occur in the root phases will be proportional to the root of the above error term.

$$\frac{\Delta\theta_e}{\theta_i} = C \sqrt{e_N^2} \log_{10} \left( \frac{\sigma_{L+1}}{\sigma_L} \right) \quad (2.44)$$

To ensure that the root phase adjustment,  $\Delta\theta_e$ , is loosely bound to prevent overcompensation, it is preferred to normalize the Frobenius norm, which is given by

$$e_N^2 = \sum_{i=r+1}^p \lambda_i / \sum_{i=1}^p \lambda_i .$$

The estimated SNR of the partitioned right matrix  $\mathbf{V}_N$  is then

approximately given by  $\frac{\sigma_{L+1}}{\sigma_L}$ , and the logarithm is taken since one does not want to

unduly scale the adjustment dramatically, especially when the observed SNR or coherence is high. Similarly, when the process is operating in poor SNR conditions, there is no real need to perform adjustments at all. Also, a fixed scaling constant is required that appears to be code dependent. Thus, one would apply (2.44) to adjust the candidate root phase only when  $\hat{L} > 1$ .

## 2.10 TOA Estimation of Maximum Length Shift-Register Sequences

In her research, Dumont [17, 18] applied the root-MUSIC algorithm to improve TOA estimation in multipath environments by processing a deterministic signal

consisting of maximum length shift-register codes. Multipath simulations were initially conducted for sequence lengths of  $P$  and the process was eventually transferred to an indoor environment to verify the TOA improvement using super-resolution. Estimated baselines were compared with measured baselines for results obtained by a typical oversampled correlator and the super-resolution method.

The reference MLSR code utilized was of period  $P = 2^7 - 1$ , with generator polynomial  $g(p) = p^7 + p^6 + 1$  (initialized at zero). The symbol period was assumed to be 100 ns and the sample frequency to be 40 MHz. The SNR was then swept through the range [-20 dB, 30 dB] in 1 dB intervals, where 200 trial runs are performed for each SNR level. The mean result per decibel interval are then displayed in Figures 2.13 - 2.21, where  $\tau_e$  denotes the corresponding time error.

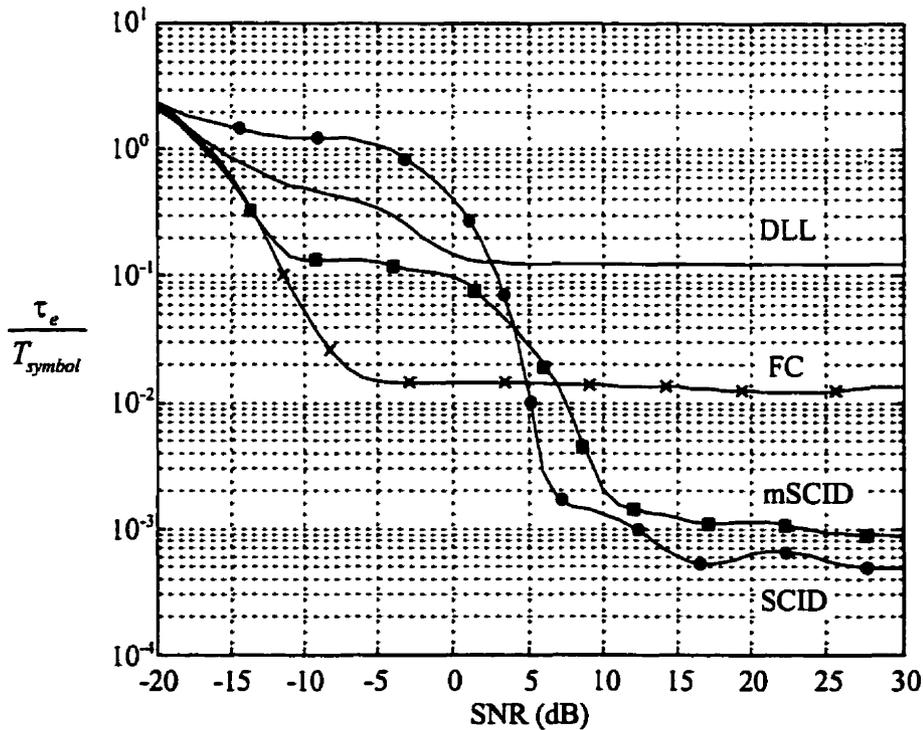


Figure 2.13. LOS TOA error for the single source case, with error normalized to the symbol period.

Fig. 2.13 compares various methods of TOA estimation for a single source case in complex additive white Gaussian noise (AWGN). The delay lock loop (DLL) utilizes an early-late gate separation of  $T_{symbol}/2$ . The frequency based correlator (FC) is also utilized for the coarse estimate of the arrival time, which can be adjusted for both the SCID and the mSCID processes. The SCID process obtains better performance at the higher SNR levels due to the slightly larger utilized bandwidth (i.e.  $N$ ). The SCID process bandlimits the frequency mapped data to approximately 90% of the null-to-null width of the correlation lobe, whereas the mSCID process uses a reduced bandwidth of approximately 80% of the null-to-null to maintain better matrix conditioning for the singular value decomposition. It is evident that the mSCID method has a reduced signal threshold level over its counterpart mainly due to the candidate root selection process being confined to a phase corridor on the complex plane. The degradation of the SCID method is further compounded by the mode overestimation.

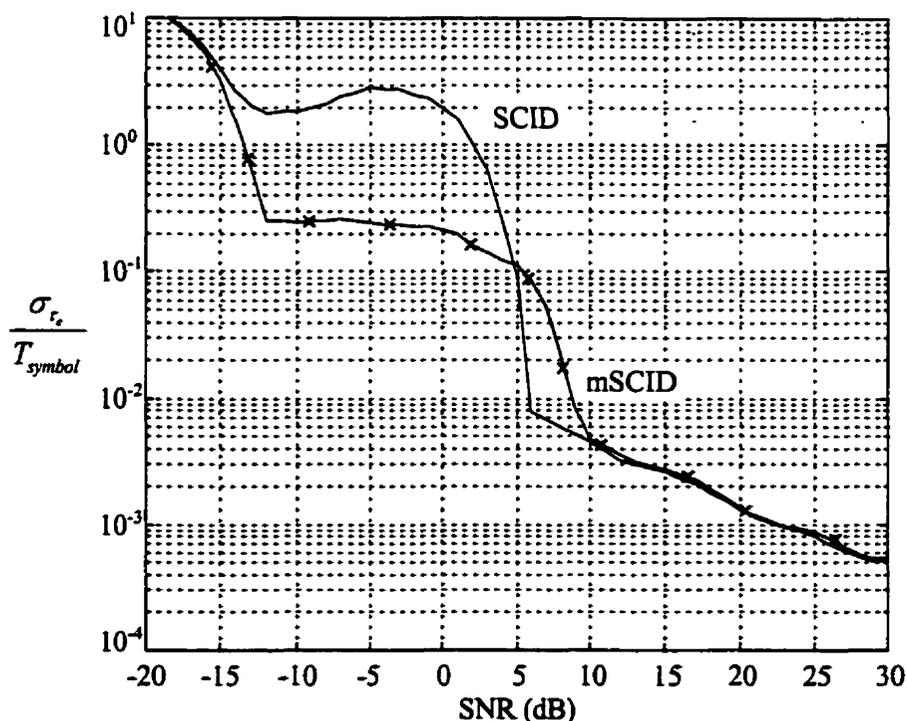


Figure 2.14. Standard deviation of LOS estimation, normalized to the symbol period.

The performance comparison is now taken to a two source scenario, where both the LOS component and the multipath component are of equal magnitude; i.e.  $\alpha_1 = \alpha_2 = e^{j\theta}$ , and the relative delay separation,  $\Delta\tau_{12}$ , between the components is varied from  $1/2$  to  $1/32$  of a symbol period.

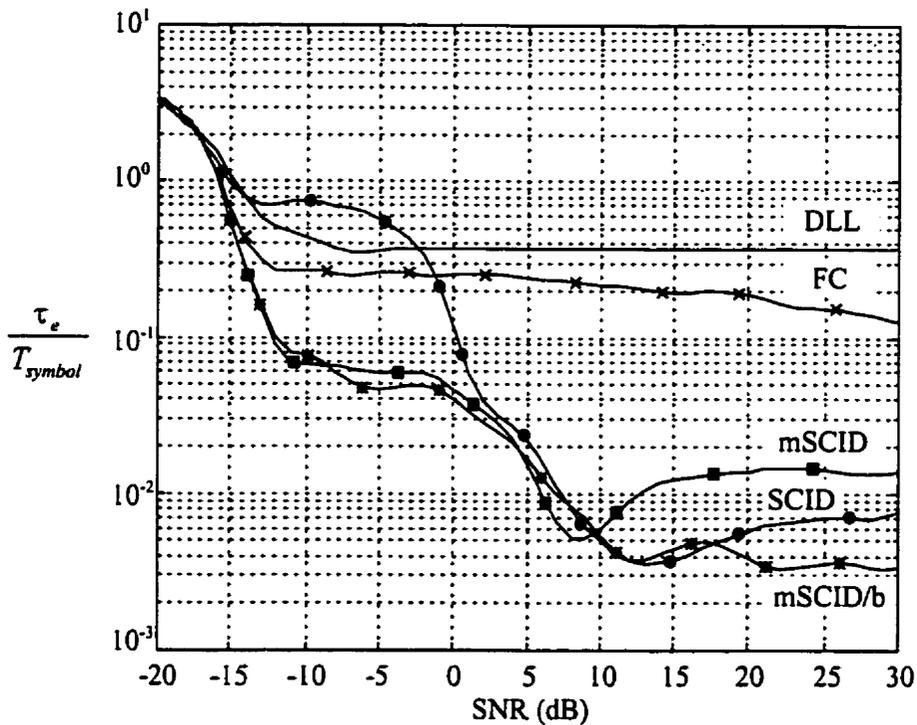


Figure 2.15. LOS TOA error for  $\Delta\tau_{12} = \frac{T_{symbol}}{2}$ .

It should be noted in Fig. 2.15 that the mSCID process is adjusted with the bias estimate of the generated source root phase, denoted as mSCID/b. This bias estimation/adjustment is not performed on mode estimates of  $\hat{L} = 1$ , since one cannot reliably ascertain whether the relative phase value has overestimated or underestimated the source. The decrease in the estimation error for both the SCID and mSCID processes in the SNR vicinity of 10 dB occurs from the matrix conditioning of the smoothed data matrix, i.e.  $\kappa(\mathbf{A})$ . This is due to the fact that as the SNR decreases, the value  $\kappa(\mathbf{A})$

linearly decreases with it, with the additive noise soon beginning to degrade the reduced rank solution.

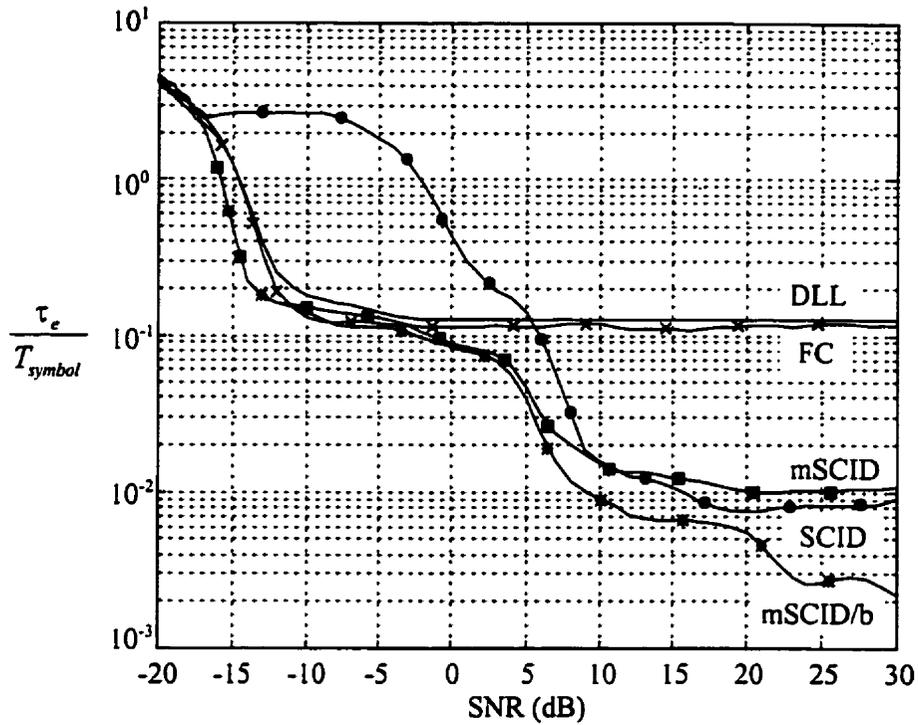


Figure 2.16. Non-LOS TOA error for  $\Delta\tau_{12} = \frac{T_{symbol}}{2}$ .

Figures 2.17 - 2.19 illustrate the SCID and mSCID LOS estimator performance for varying relative delay separations, where the relative delay separation is now denoted as

$$\Delta\tau_N = \frac{\Delta\tau_{12}}{T_{symbol}}$$

the estimator performance for relative delay separations less than  $T_{symbol}/2$ , the mode estimation routine fails to detect both sources. Hence, a single source root pair is generated, which is typically located at the phase midpoint of the expected source root locations. There are regions where the TOA estimator improves as the SNR decreases, where the non-principal singular values increase in magnitude due to the additive noise.

This allows the mode estimator process in the root-MUSIC algorithm to either correctly determine the number of sources, or overestimate the number of sources.

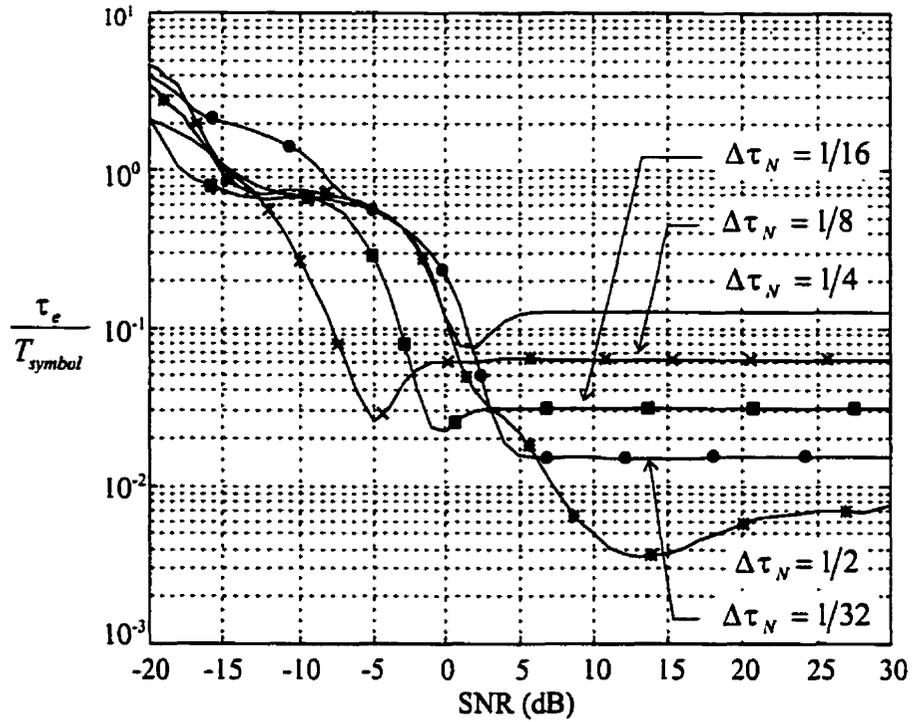


Figure 2.17. SCID LOS estimation error for varying  $\Delta\tau_N$ .

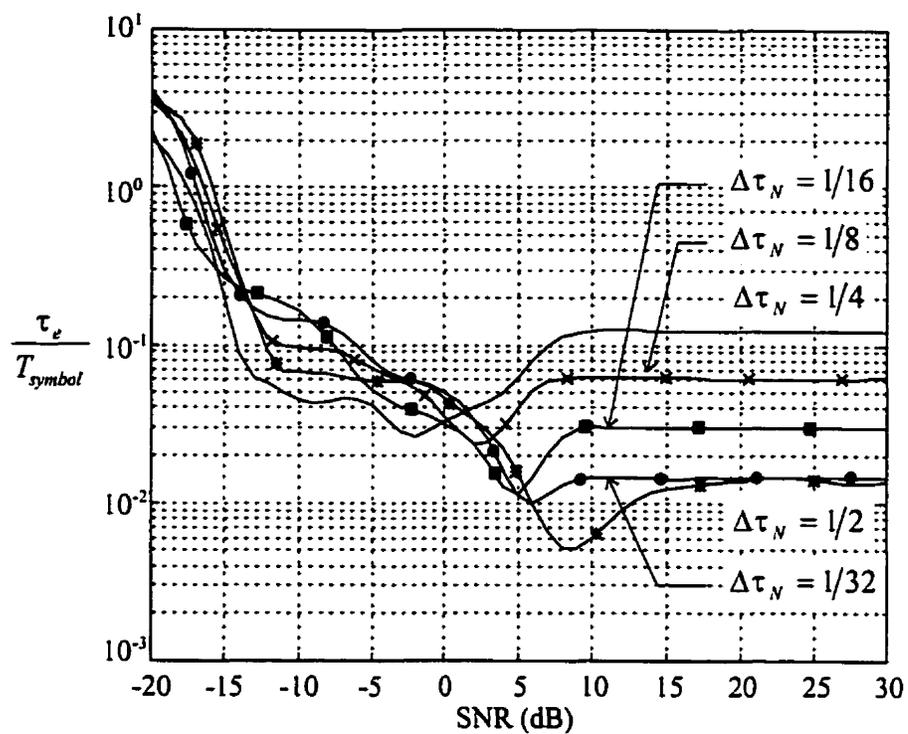


Figure 2.18. mSCID LOS estimation error for varying  $\Delta\tau_N$ .

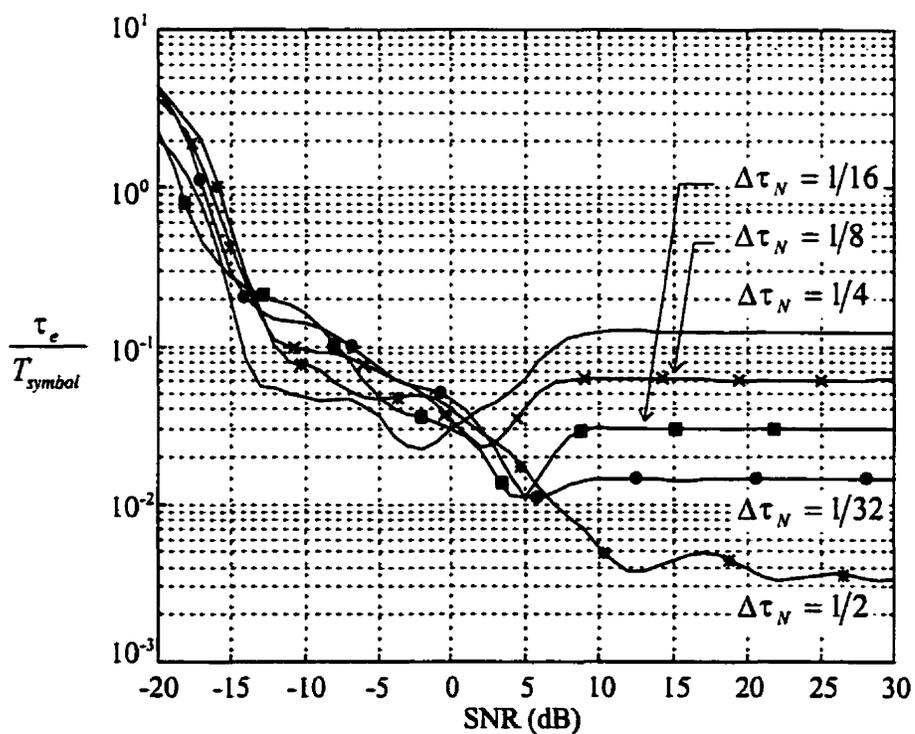


Figure 2.19. mSCID/b LOS estimation error for varying  $\Delta\tau_N$ .

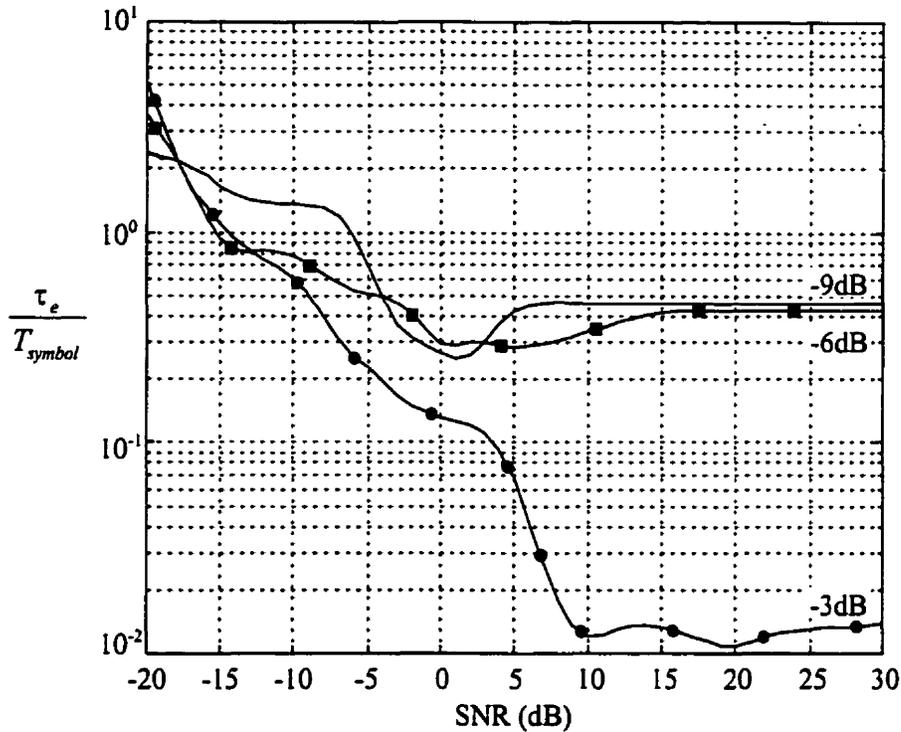


Figure 2.20. SCID LOS TOA error for varying LOS magnitude relative to the multipath component, with  $\Delta\tau_{12} = \frac{T_{symbol}}{2}$ .

Figures 2.20 and 2.21 provide estimation results for a fixed relative delay between the LOS and multipath components, with the magnitude of the LOS component being varied with respect to the non-LOS component, i.e.  $20 \log_{10}(\alpha_1/\alpha_2) = \{-3\text{dB}, -6\text{dB}, -9\text{dB}\}$ . Although the source separation does not exceed the lower coherence bound for the FBS method, the resultant estimates are strongly influenced by the dominant multipath component, especially when the candidate roots are determined wholly by a magnitude criteria. The bias adjusted mSCID values are not illustrated here since there is little difference then with the mSCID plots shown in Fig. 2.21. This is with the exception of the -3 dB relative magnitude plot. Otherwise, there are only minor regions where TOA estimator improvement occurs, i.e. where  $\hat{L}$  is nearly estimated properly.

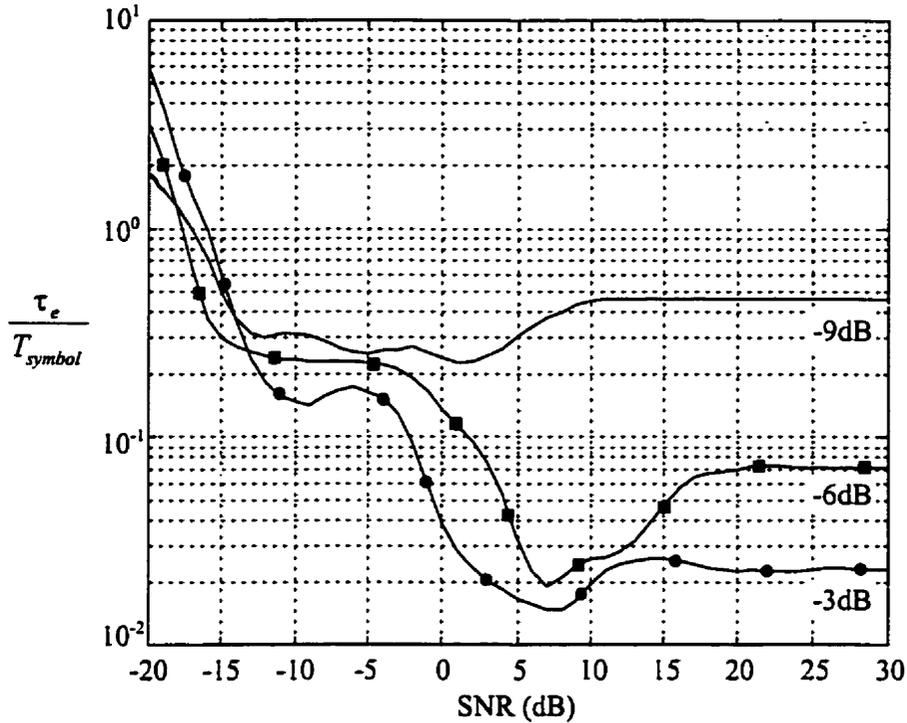


Figure 2.21. mSCID LOS TOA error for varying LOS magnitude relative to the multipath component, with  $\Delta\tau_{12} = \frac{T_{symbol}}{2}$ .

### 2.11 Indoor Baseline Estimation

In the past, Dumont [17, 18] obtained indoor channel measurements at *TRLabs* in Calgary using AGT's Impulse Response Identification System (IRIS) [53]. Baseline measurements were estimated using both the methods of frequency-domain based correlation (FC) and super-resolution processing (SCID).

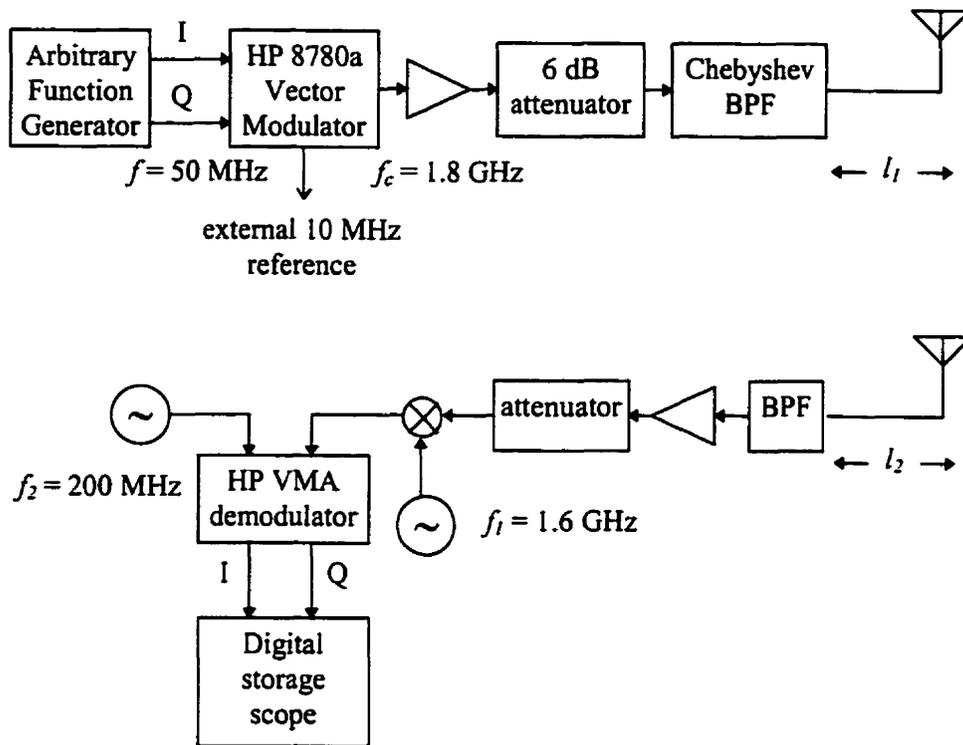


Figure 2.22. IRIS transmitter - receiver block diagram.

In those measurements, an arbitrary function generator (LeCroy AFG model 9109) was used to transmit a PN sequence of length  $P = 127$ . The LeCroy AFG generated four output samples per chip interval for a 50 MHz chip rate obtained from a dual channel 8 bit digital-to-analog converter. This chip rate was chosen by Dumont due to the fact that indoor measurements were being conducted and large baselines (greater than 30 meters) could not be achieved in the selected environment. The PN sequence was then binary phase shift keying (BPSK) modulated and upconverted to 1.8 GHz using a Hewlett Packard 8780a vector modulator. The resulting wideband signal was then amplified by a power amplifier (+40 dBm compression point), passed through a 6 dB attenuator and a 6 pole passive Chebyshev BPF (with a 100 MHz bandwidth and 2 dB insertion loss). The receiver portion of the IRIS system consists of a bandpass filter and low noise amplifier. An HP adjustable attenuator precedes the downconverter to ensure that the mixer is operated in a linear region. The received signal used in these measurements was then passed through a two stage down conversion process to generate

the complex baseband outputs that were sampled and stored on a LeCroy 7200 digital storage oscilloscope (DSO) with 8 bit precision. Since it was desirable to evaluate the performance of the SCID process it was necessary to achieve system synchronization to minimize measurement errors on the absolute TOA values. This synchronization was achieved from the 10 MHz reference output of the HP 8780a vector modulator which was used to source the AFG, the two local oscillators on the receiver, and the DSO. Other parameters of the system configuration were the length and type of cabling required to physically connect the transmit and receive antennas to their associated ports. The cabling used was RG400 which has a velocity factor of 0.71, with lengths  $l_1 = 2$  m and  $l_2 = 16.5$  m.

Baseline measurements under varying environmental conditions were obtained by Dumont [17, 18] with the IRIS system, and these results are given in Table 2.2, where four epochs were recorded for each parameter variation.

Table 2.2: SCID Estimated Baselines [17]

Antenna Separation (m)	Measurement Conditions	SCID (m)	mode estimate	FC (m)
5.2	LOS	4.26	5	4.16
		3.97	6	3.86
		2.62	6	3.86
		3.99	6	3.86
11.15	LOS	9.75	8	11.35
		11.26	8	11.65
		11.10	8	11.65
		11.65	9	11.35
13.98	non-LOS, Tx antenna in office cubicle	13.90	10	14.95
		14.16	10	14.95
		14.28	10	14.95
		13.68	10	14.95
17.35	LOS	16.52	9	16.45
		16.64	9	16.45
		16.63	9	16.45
		16.64	9	16.45
24	LOS	25.40	8	24.94
		23.36	6	25.54
		23.64	6	25.54
		23.26	6	25.54
24	non-LOS, wood door between Tx and Rx antennas	26.52	7	21.25
		26.60	7	21.55
		26.64	7	21.25
		26.68	7	21.25
24	non-LOS, glass door between Tx and Rx antennas	22.52	5	21.85
		22.80	7	22.15
		22.77	5	22.15
		22.65	5	21.85

The data measurements were then reprocessed with the mSCID method. As outlined in section 2.8, the vector length of the frequency domain data was significantly reduced so

that large discontinuities in the deconvolved frequency response were minimized. This allows for improved matrix conditioning prior to decomposition.

Table 2.3: mSCID Estimated Baselines

Antenna Separation (m)	Measurement Conditions	mSCID (m)	mode estimates	FC (m)
5.2	LOS	5.02	5	4.16
		4.75	6	3.86
		4.75	6	3.86
		4.77	6	3.86
11.15	LOS	10.65	8	11.35
		11.95	8	11.65
		11.77	8	11.65
		11.76	9	11.35
13.98	non-LOS, Tx antenna in office cubicle	14.65	10	14.95
		14.88	10	14.95
		15.06	10	14.95
		14.39	10	14.95
17.35	LOS	17.30	9	16.45
		17.33	9	16.45
		17.36	9	16.45
		17.37	9	16.45
24	LOS	24.53	8	24.94
		24.64	6	25.54
		24.73	6	25.54
		24.96	6	25.54
24	non-LOS, wood door between Tx and Rx antennas	27.20	7	21.25
		27.29	7	21.55
		27.35	7	21.25
		27.45	7	21.25
24	non-LOS, glass door between Tx and Rx antennas	23.21	5	21.85
		23.50	7	22.15
		23.52	5	22.15
		23.34	5	21.85

The mean baseline estimates for Tables 2.2 and 2.3 were determined and are given below, where use of the SCID and mSCID methods has resulted in comparable values under LOS conditions.

Table 2.4: Mean Baseline Estimates

Antenna Separation (m)	Measurement Conditions	SCID (m)	mSCID (m)	FC (m)
5.2	LOS	3.96	4.82	3.94
11.15	LOS	10.94	11.53	11.50
13.98	non-LOS (office cubicle)	14.01	14.74	14.95
17.35	LOS	16.61	17.34	16.45
24	LOS	23.92	24.72	25.39
24	non-LOS (wood door)	26.61	27.32	21.33
24	non-LOS (glass door)	22.69	23.39	22.00

It may be noticed that both processes have overestimated the baseline when the transmission path was obscured by a wood door. Thus, one can surmise that the arrivals were closely spaced in time, and the LOS component had a reduced relative magnitude.

## **Chapter 3: Concepts of North American Cellular and Geolocation Systems**

### **3.1 North American Cellular Radio Architecture**

With AT&T's (formally Bell Systems) commercial deployment of cellular radio in 1975 after extensive testing in the Chicago area, cellular radio has become the fastest growing field of electronic communication. It is estimated that there are over 69 million cellular subscribers in North America as of December 1998, and 11.2 million new subscribers were added to the North American market in 1997 alone [54]. Due to these increased capacity demands in populated areas, the CTIA adopted a proposal to expand system capacity by changing the analog system to a fully digital system. However, due to the extensive costs of immediately implementing a new network architecture the CTIA opted to convert the existing network over several stages with the analog portion eventually being phased out. This transition is accomplished by modifying existing base station equipment to handle both analog and digital subscribers, hence, allowing wireless carriers to switch analog channels to digital channels as the analog network reaches capacity due to subscriber demands.

The Advanced Mobile Phone Service (AMPS) is the analog system used in North America, and the digital cellular technology (first generation) is the interim standard IS-54-B [13]. AMPS uses the method of frequency division multiple access (FDMA), where the signal consists of modulated speech, supervisory audio tones (SAT), signaling tone (ST), and wideband data (WBD). The SAT is primarily used to distinguish the signal of interest (SOI) from the cochannel interference and can be one of three frequencies: 5970 Hz, 6000 Hz, 6030 Hz. The ST is used as a pre-amble or post-amble to indicate specific network signaling features (e.g. data messaging via WBD on an assigned voice channel), alerting the subscriber of an incoming call, handoffs, or call termination. If one neglects filtering requirements, the AMPS passband signal can be represented as follows:

$$s(t) = \begin{cases} \text{Re}\left\{e^{j\omega_c t + j2\pi\beta f_m \int v(t) dt + jk_1 \sin(2\pi f_{SAT} t)}\right\}, & \text{voice channel only} \\ \text{Re}\left\{e^{j\omega_c t + jk_1 \sin(2\pi f_{SAT} t) + jk_2 \sin(2\pi f_{ST} t)}\right\}, & \text{voice channel only} \\ \text{Re}\left\{e^{j\omega_c t + jk_3 x_{WBD}(t)}\right\}, & \text{voice channel or control channel} \end{cases} \quad (3.1)$$

where  $\omega_c$  is the angular carrier frequency,  $\beta$  is the speech modulation index,  $f_m$  is the upper passband edge of the bandlimited speech  $v(t)$ , and where  $f_{SAT}$  and  $f_{ST}$  are the SAT and ST frequencies, respectively. The Manchester encoded data is denoted as  $x_{WBD}(t)$ , and  $k_i$  in Equation 3.1 represents the associated modulation indices given in the table below.

Table 3.1 Modulation Indexes for AMPS

parameter	frequency component	modulation index (nominal)
$\beta$	speech	3
$k_1$	SAT	1/3
$k_{2,3}$	ST or WBD	0.8

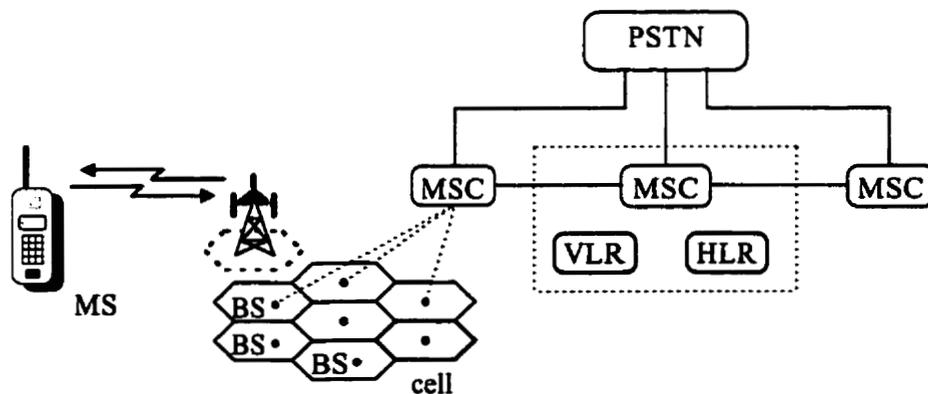


Figure 3.1. Wireless and wired connectivity of CMRS.

In general, the operations of the CMRS system can be explained as follows.

The mobile station (MS) initially obtains connectivity to the Mobile Switching Center (MSC) via the base station (BS). The wireless subscriber's billing account is geographically defined such that all necessary subscriber information is contained in the Home Location Registry (HLR), thus any incoming calls utilize the HLR information for further appropriate routing. When the subscriber leaves the coverage zone of their designated HLR they are classified as a *roamer*, and the network must determine if the roaming subscriber has a legitimate billing account and if so, must then set up a temporary address database entry in the Visitor Location Registry (VLR). The VLR will then pass required information to the subscriber's HLR to maintain seamless telephone service under the assigned mobile identification number (MIN) and electronic serial number (ESN) to which any incoming calls are routed to the appropriate BS. The net functionality of the MSC is to administer the radio frequency channels allocated to the CMRS (e.g. AMPS, IS-54-B), coordinate the designated BS and the subscribers, and maintain the integrity of the network.

In 1974, the FCC had allocated a 40 MHz band in the 824 - 894 MHz frequency region for mobile radio usage, where this allocated band was equally divided into mobile transmit bands and mobile receive bands. Subsequently, this spectrum was further subdivided for two separate carriers: the radio common carrier (RCC, non-wireline or A side) and wireline common carrier (WCC, wireline or B side). The wireline common carrier is a service provider that also offered wireline services to its customers. This allowed for 333 frequency division duplexed (FDD) channels per carrier. Due to traffic congestion; even when wireless carriers performed cell splitting to increase channel capacity for an ever increasing subscriber base, the FCC had to expand the mobile radio bandwidth by an additional 10 MHz with the wireline and non-wireline carriers each receiving an additional 5 MHz which was again equally split into transmit and receive bands. This resulted in an additional 83 FDD channels per carrier, designated as A' (1.5 MHz), A'' (1 MHz), and B' (2.5 MHz) as illustrated in Fig. 3.2.

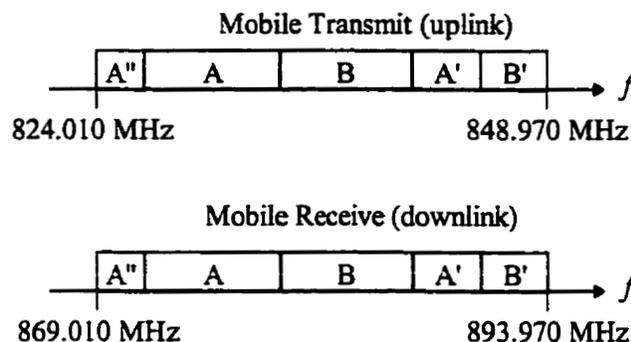


Figure 3.2. Frequency allocation for Enhanced AMPS.

Among the net 832 FDD channels, 42 are designated as control or setup channels, while the remaining 790 are designated as voice channels and traffic channels.

Typically as wireless voice traffic increases, the wireless carriers perform cell splitting to maintain the same service quality and thus the initial larger cell is split into smaller cells and the frequency channel assignments reorganized to account for this. Immediate benefits of this operation are reduced transmit power levels from the base station equipment and also reduced transmit levels for the wireless terminals (telephones), which extends their battery life. The frequency reuse pattern utilized by wireless carriers is based upon a polygon series rather than a circular pattern which gives maximum coverage for a given cell radius, and in turn generates the greatest physical separation from adjacent cell centers. This physical separation is then used to determine the amount of adjacent channel interference and cochannel interference. If the radiation patterns used in the frequency reuse plan were circular, then there would be significant overlap between adjacent cells as well as significant dead spots of radio reception, thus implying that additional cell sites would be required for total coverage. However, measurements in the real world have shown that the signal strength contours from point source emissions at cell centers have distorted shapes, but are near enough in design to the initial polygon series.

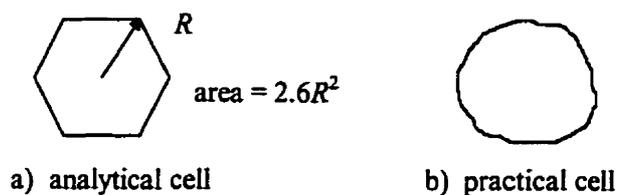


Figure 3.3. Illustration of hexagonal cell and practical cell having uniform received signal strength at the cell boundaries.

Each cell is then assigned one of the 21 possible control channels reserved per carrier and a set of voice channels. The distribution of the channels must then follow a well established frequency reuse plan to minimize network self interference. The most widely used frequency reuse plan is a  $N = 7$  cell cluster as shown in Fig. 3.4. The 416 channels would then be evenly distributed in the cell cluster, allowing approximately 59 channels per cell. This pattern would then be repeated throughout the cellular geographical service area (CGSA).

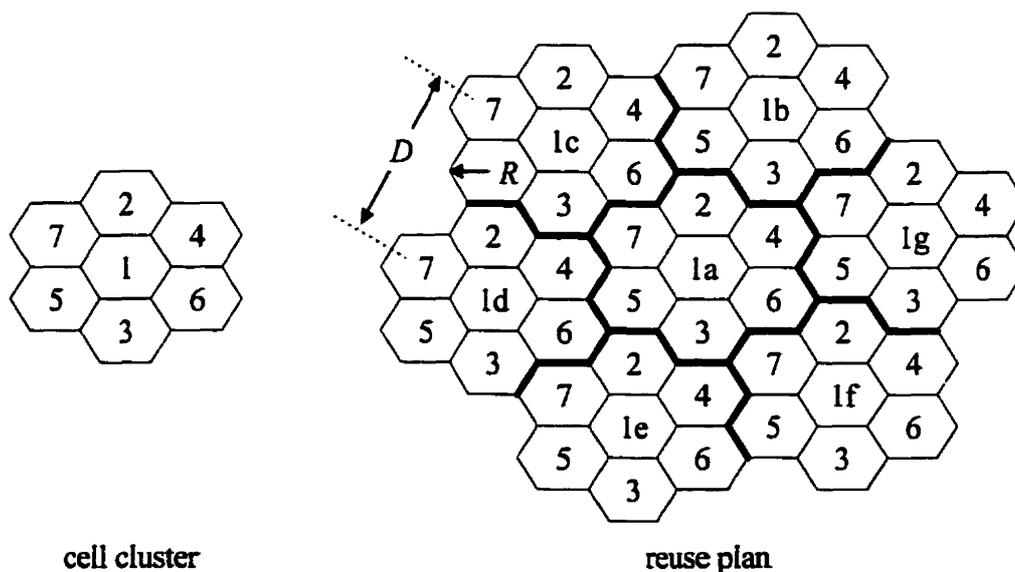


Figure 3.4. Illustration for frequency reuse plan of  $N = 7$ .

The cochannel distance or reuse distance,  $D$ , is given by  $D = \sqrt{3N}R$ , where  $N$  is the cell cluster size adopted in the frequency plan, and  $R$  is the cell radius. This parameter is then used to estimate the cochannel interference. For the illustration in Fig. 3.4, the cochannel distance is  $D = \sqrt{21}R$ .

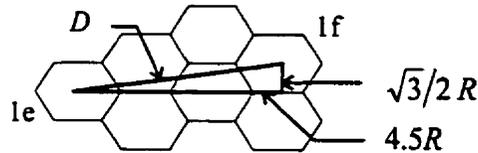


Figure 3.5. Illustration of cochannel distance for  $N = 7$ .

For equal power transmissions from the cell centers (i.e. omni-directional antennae), for both the desired cell and the cochannel cell, the worst case signal-to-interference ratio (SIR) may be approximately calculated using

$$\frac{S}{I} \approx 10 \log \left\{ \left[ \frac{D-R}{R} \right]^n \right\}, \quad (3.2)$$

where  $R$  denotes the cell radius,  $D$  is the distance to the cochannel emitter (i.e. a BS), and  $n$  is the propagation decay law. The propagation decay law varies per radio environment, but is typically  $2 \leq n \leq 5$ . As an example, for the seven cell reuse pattern illustrated above, the worst case scenario would be for six cochannel cells, resulting in a signal-to-interference ratio (first tier) given by

$$\frac{S}{I} \approx 10 \log \left\{ \left[ \frac{D-R}{R} \right]^n \right\} - 10 \log(6).$$

Although a seven cell layout is the norm for frequency reuse planning there are more efficient reuse patterns to increase channel capacity as well as increase the network SIR [55, 56]. It may be noted that the AMPS system has a qualitative minimum SIR of 18 dB.

Another approach to minimize the cochannel interference is the method of discontinuous transmission (DT<sub>x</sub>), which takes advantage of the fact that statistically a subscriber will speak for approximately one third of the conversation. Hence, the transmitter may reduce the output power or power down completely during quiet periods for the analog mode or digital mode, respectively. This improves the network quality in terms of cochannel interference and has the added benefit of extending the handset's battery talk time.

### **3.2 IS-54-B Air - Network Interface**

The multiple access control (MAC) for cellular subscribers was originally based on the EIA/TIA-553 Mobile Station - Land Station Compatibility Specification [57]. As pointed out in Chapter 1, it was assumed that analog cellular would be phased out within a few years of the deployment of digital cellular, so the interface standards were modified slightly to accommodate analog, digital, and dual capable (referred to as dual-mode) cellular telephones during this period. These revisions are known as the EIA/TIA Interim Standard IS-54-B. The network outlined by this standard is able to identify the type of cellular telephone (analog or digital) attempting to gain network access by specific fields embedded in Reverse Control Channel (RECC) messages.

Whenever a subscriber originates a call, receives a call (pages), power cycles the cellular telephone, or autonomously registers (timer based method), a 10 kbps  $\pm$  1 bps Manchester encoded message is sent on the RECC in acknowledgment to overhead messages sent by the serving base station on the Forward Control Channel (FOCC). The Manchester encoded data (i.e. WBD) contains 36 data bits per word which is block encoded into 48 bit words with a shortened (63,51;5) Bose-Chaudhuri-Hocquenghem (BCH) code sent on a FM modulated carrier with a  $\pm$  8 kHz deviation. The encoded word is then repeated five times (called a word block), so that consecutive bit errors from

the fading channel will not occur over all repeats. Thus, three out of five majority voting is conducted at the receiver which achieves reliable word reception.

Each RECC message contains a deterministic preamble, which is called the seizure precursor. The seizure precursor consists of a 30 bit ‘...1010...’ dotting pattern used for receiver clock synchronization, a word sync which is an 11 bit Barker code [11100010010] that is used for signal detection and word framing, and the coded Digital Color Code (DCC) which is used to identify and aid rejection of cochannel interference that comes from the cellular carrier’s adopted frequency reuse pattern.

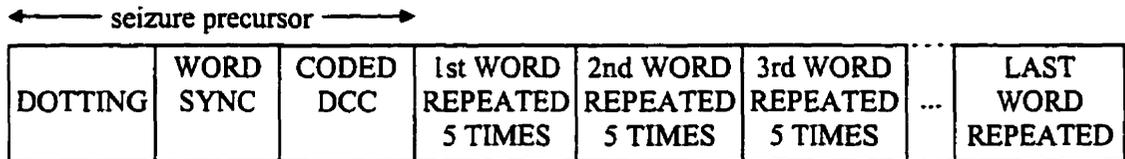


Figure 3.6. Mobile Station - to - Base Station (RECC) message format.

The Barker codes are sometimes called perfect codes because the highest normalized correlation sidelobe at zero Doppler frequency consists of only a single code element, i.e.  $P^{-1}$ , where  $P$  is the code length of the binary Barker code.

Once the RECC message stream has been decoded by the base station, the words are broken down into their respective field identifiers. This message stream can contain combinations of one to six of the following words.

## Word A: Abbreviated Address

F=0	NAWC	T	S	E	ER	SCM <sub>3-0</sub>	MIN <sub>1 23-0</sub>				P
1	3	1	1	1	1	4	24				12

## Word B: Extended Address

F=0	NAWC	LOCAL	ORDQ	ORDER	LT	EP	SCM <sub>4</sub>	MPC	SDCC <sub>1</sub>	SDCC <sub>2</sub>	MIN <sub>2 33-24</sub>	P
1	3	5	3	5	1	1	1	2	2	2	10	12

## Word C: Serial Number

F=0	NAWC	Electronic Serial Number (ESN)									P
1	3	32									12

## Word C: Authentication

F=0	NAWC	COUNT	RANDC			AUTHR			P
1	3	6	8			18			12

## Word C: Unique Challenge Order Confirmation

F=0	NAWC	RSVD = 00...0					AUTHU			P
1	3	14					18			12

## Word C: Base Station Challenge

F=0	NAWC	RANDBS									P
1	3	32									12

## Word D: Called Address (first word)

F=0	NAWC	DIGIT <sub>1</sub>	DIGIT <sub>2</sub>	DIGIT <sub>3</sub>	DIGIT <sub>4</sub>	DIGIT <sub>5</sub>	DIGIT <sub>6</sub>	DIGIT <sub>7</sub>	DIGIT <sub>8</sub>	P
1	3	4	4	4	4	4	4	4	4	12

## Word D: Called Address (second word)

F=0	NAWC	DIGIT <sub>9</sub>	DIGIT <sub>10</sub>	DIGIT <sub>11</sub>	DIGIT <sub>12</sub>	DIGIT <sub>13</sub>	DIGIT <sub>14</sub>	DIGIT <sub>15</sub>	DIGIT <sub>16</sub>	P
1	3	4	4	4	4	4	4	4	4	12

Figure 3.7. RECC word formats.

The bit field identifiers for the previous words are defined as follows.

Table 3.2 RECC Data Fields

<u>Data field</u>	<u>Data interpretation</u>
F	First word identifier. It is set to '1' in the first word and '0' in all other words.
NAWC	Number of Additional Words Coming in a three bit BCD format.
T	Origination/response field. The message was sent as an origination or an order if this field was set to '1'; otherwise the message is identified as an order response or page response.
S	Send serial number. The serial number (word C) is sent in the RECC message when this field is set to '1'.
E	Send extended address. The extended address (MIN <sub>2</sub> ) is sent in the RECC message when this field is set to '1'.
ER	Extended Protocol Reverse Channel. This bit indicates if the current message is using the extended protocol format.
SCM <sub>4-0</sub>	Station Class Mark. This field identifies characteristics of the cellular telephone (analog or digital capable), see Table A1.
MIN <sub>1</sub>	First part of the Mobile Identification Number. It contains the seven digit cellular telephone number encoded into 24 bits.
P	Bose-Chaudhuri-Hocquenghem parity.
LOCAL	Local control. This field is specific to each wireless carrier, see Table A2.
ORDQ	Order Qualifier. Qualifies the order confirmation to a specific action, see Table A2.
ORDER	Order field. Identifies the order type, see Table A2.
LT	Last Try indicator.
EP	Extended protocol. This bit indicates to the network if the cellular telephone is capable of using the extended protocol.
MPCI	Mobile Phone Class Identifier, see Table A3.
SDCC <sub>1</sub>	Supplementary Digital Color Codes.
SDCC <sub>2</sub>	Supplementary Digital Color Codes.
MIN <sub>2</sub>	Second part of the Mobile Identification Number. Contains the three digit area code for the cellular telephone encoded into 10 bits.
ESN	Serial number field.
COUNT	A modulo 64 counter used for authentication and anti-fraud purposes.
RANDC	A 8 bit number used to confirm the last random challenge received (used for anti-fraud).
AUTHR	Output of the Cellular Authentication, Voice, and Encryption (CAVE) algorithm.
AUTHU	Output of the CAVE algorithm when responding to a specific base station challenge.
RANDBS	A random number used in the authentication and anti-fraud process.
DIGIT	Called digit field in a four bit BCD format.

Table 3.3 Mobile Station Power Levels

Power Level	Nominal ERP (dBW) for Mobile Station Class							
	I	II	III	IV	V	VI	VII	VIII
0	6	2	-2	-2	*	*	*	*
1	2	2	-2	-2	*	*	*	*
2	-2	-2	-2	-2	*	*	*	*
3	-6	-6	-6	-6	*	*	*	*
4	-10	-10	-10	-10	*	*	*	*
5	-14	-14	-14	-14	*	*	*	*
6	-18	-18	-18	-18	*	*	*	*
7	-22	-22	-22	-22	*	*	*	*
8	-22	-22	-22	-26 ± 3dB	*	*	*	*
9	-22	-22	-22	-30 ± 6dB	*	*	*	*
10	-22	-22	-22	-34 ± 9dB	*	*	*	*

It should be noted that

- Classes V, ..., VII have been reserved for future definition by the CTIA,
- Class IV is a dual-mode cellular telephone,
- Only mobile stations assigned to a digital traffic channel may operate below power level 7.

The initial approach for position location of cellular telephones was based upon an established digital voice channel (i.e. traffic channel), since it was expected at the beginning of the research period that most wireless carriers would adopt a fully digital cellular network. However, due to varying subscriber densities and voice quality of the full rate codecs used in IS-54-B, the digital traffic channel (DTC) feature of the dual-mode cellular base stations were turned off in some regions, e.g. Telus Mobility had inhibited the DTC feature for a significant period of time. Presently, wireless carriers are looking at the GSM and CDMA standards as alternatives to IS-54-B as channel capacity is virtually the same (if not better) and there is a noticeably improved voice quality. Since the RECC message contains an *a priori* known sequence, the seizure precursor, this sequence was utilized in a single event positioning method [58, 59].

### 3.3 North American Digital Cellular Radio (IS-54-B)

The North American Digital Cellular (NADC) system operates in the existing frequency bands and channels specified for AMPS. The system was designed to provide a transition from the current analog system to a fully digital system. The control channels remain the same as for AMPS, however, the differences occur on the voice channels. The speech is sampled and digitized to obtain 64 kbps PCM data. This PCM data is then compressed to 16.2 kbps via a vocoder, interleaver, and half rate convolutional coder. Because of capacity limitations in dense metropolitan areas, another fully digital standard, IS-136 [60] is being deployed. The EIA/TIA Interim Standard IS-136 increases the efficiency of the traffic volume, adds enhanced subscriber features, and extends handset battery life by utilizing digital control channels (DCCH) rather than the analog control channels used in AMPS and IS-54-B.

The modulation method chosen for the NADC standard is  $\pi/4$  shifted differentially encoded quadrature phase shift keying ( $\pi/4$  - DQPSK). One of the benefits that is easily seen from the constellation diagram (Fig. 3.8) is that the transitions never pass through the origin, therefore, the modulated signal has reduced envelope fluctuations which aids the carrier and clock recovery mechanisms. This also makes the system less sensitive to the nonlinearities of power amplifiers, allowing class-AB power amplifiers to be used in the transmitter.

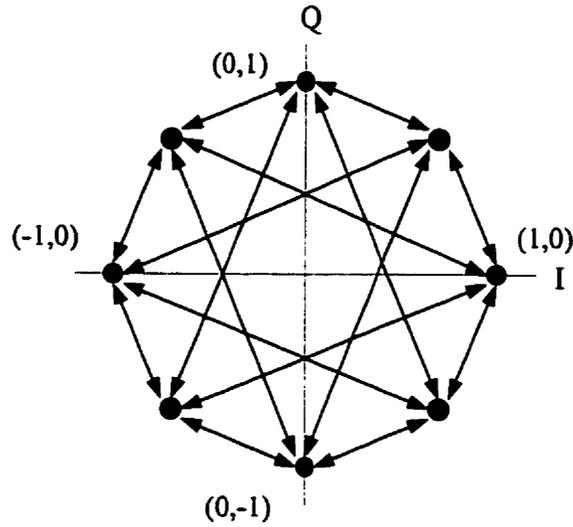


Figure 3.8. Constellation diagram for  $\pi/4$  - DQPSK modulation.

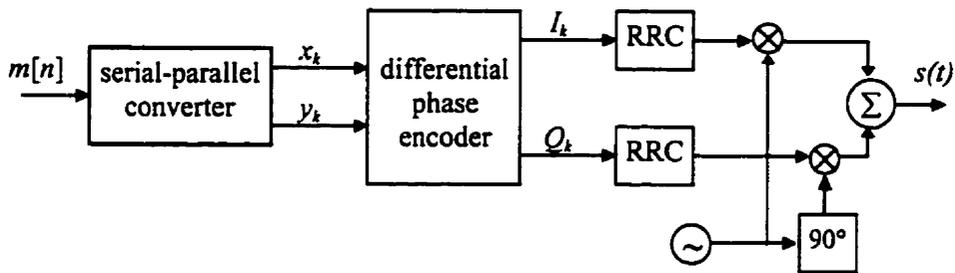


Figure 3.9. Block diagram of  $\pi/4$  - DQPSK modulator.

The 48.6 kbps message data stream,  $m[n]$ , entering the modulator is split into two parallel data streams  $x_k$  and  $y_k$ , where all odd numbered bits of  $m[n]$  form the  $x_k$  data stream and all even numbered bits form the  $y_k$  data stream. The split data streams are then differentially phase encoded, where memory is introduced by previous symbol amplitudes to produce the following output sequences:

$$\begin{aligned} I_k &= I_{k-1} \cos(\Delta\Phi(x_k, y_k)) - Q_{k-1} \sin(\Delta\Phi(x_k, y_k)) \\ Q_k &= I_{k-1} \sin(\Delta\Phi(x_k, y_k)) + Q_{k-1} \cos(\Delta\Phi(x_k, y_k)). \end{aligned} \quad (3.3)$$

The dibit encoded phase changes ( $\Delta\Phi$ ) are defined as follows.

Table 3.4 Differential Phase Encoding

$x_k$	$y_k$	$\Delta\Phi$
0	0	$\pi/4$
0	1	$3\pi/4$
1	1	$-3\pi/4$
1	0	$-\pi/4$

The corresponding output sequences  $\{I_k, Q_k\}$  can then take on one of eight possible states:  $(0, \pm 1)$ ,  $(\pm 1, 0)$ ,  $(\pm 1/\sqrt{2}, \pm 1/\sqrt{2})$ , generating the constellation diagram in Fig. 3.8.

The two pulse amplitudes are then applied to baseband square root raised cosine filters (RRC), which are specified by a roll-off factor  $\alpha = 0.35$  and symbol duration of  $T \cong 41.15\mu s$ . The RRC filter outputs are then frequency translated to the designated channel frequency. The resultant signal  $s(t)$  is then given by:

$$s(t) = \sum_n g(t - nT) \cos \Phi_n \cos(\omega_c t) - \sum_n g(t - nT) \sin \Phi_n \sin(\omega_c t), \quad (3.4)$$

where  $g(t)$  is the impulse response of the designated baseband filters,  $\omega_c$  is the assigned carrier angular frequency,  $T$  is the symbol duration, and  $\Phi_n$  is the accumulated phase at the  $n^{\text{th}}$  symbol interval given by

$$\Phi_n = \Phi_{n-1} + \Delta\Phi_n, \quad (3.5)$$

where the phase change  $\Delta\Phi_n$  was previously defined in Table 3.4.

It should be noted that the encoder/modulator block diagram outlined in Fig. 3.9 is not sufficient for actual system operation since additional filtering requirements are necessary to ensure intermodulation products and spurious emissions are kept below levels outlined in the EIA/TIA Interim Standards. This encoder/modulator block diagram, however, does show the basic functionality.

### 3.4 RECC Time-of-Arrival Processing

Klukas *et al.* [58, 59] demonstrated the ability of positioning a "pseudo" phone via the mSCID process, where the entire seizure precursor is used as the reference code sequence. An actual phone was not utilized to ensure that degradation would not occur to the wireless service provider's network. The pseudo phone had all the hardware traits and emission requirements as outlined in EIA/TIA standards, but only performed RECC transmissions on an isolated channel. Hence, the pseudo phone would transmit on an idle boundary control channel, i.e. channel 334, which corresponded to a carrier frequency of 835.020 MHz. The general receiver architecture of Cell-Loc's prototype listening station (LS) [59], Cellocate™, is illustrated below.

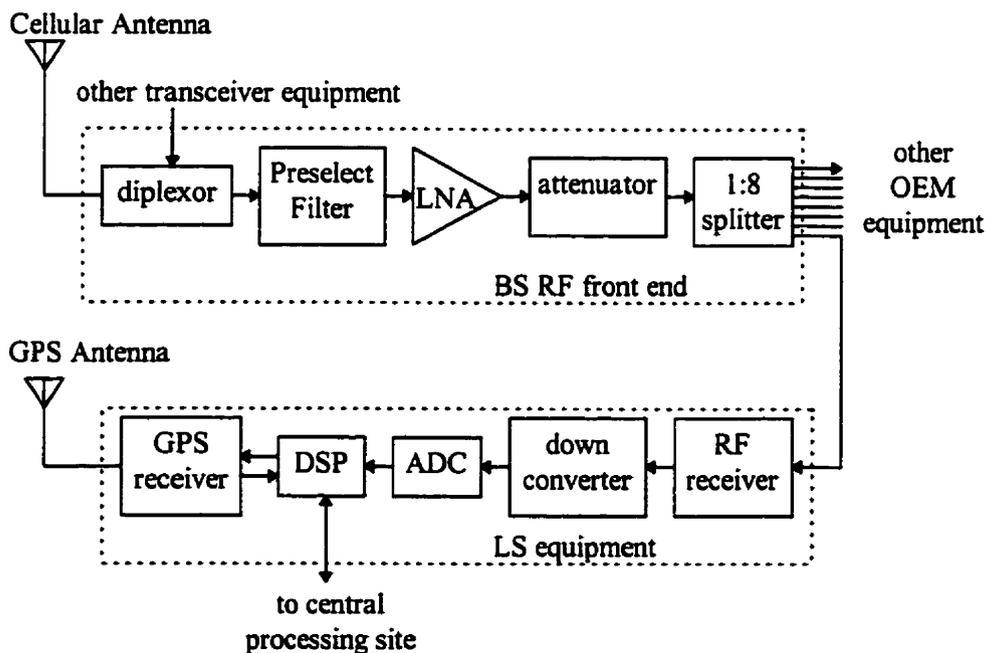


Figure 3.10. Block diagram of RECC Listening Station equipment.

The LS equipment interfaces to the wireless carrier's RF front-end equipment via one of the available ports on a multicoupler. This allows the system to utilize the elevated antennas and available gain, which further reduces deployment costs. The LS receiver performs narrowband isolation, down conversion, amplification, filtering, and

demodulation of the frequency shift keyed (FSK) RECC messages. The received baseband signal is then sampled and stored for additional signal processing. The GPS receiver operates in time transfer mode, which provides a method of wide-area system clock synchronization among the deployed listening stations and allows the use/generation of event time markers.

The RECC access attempts are typically single bursts lasting approximately 100 ms in duration and are performed at a power level setting of two (see Table 3.3). This gives adequate received signal strength at multiple listening stations, which are co-located with the BS equipment in adjacent cell sites. Once the RECC access attempt is detected, the observation is stored via a circular buffer and referenced with respect to GPS time. This provides the coarse estimate of the absolute TOA (including hardware lags). The stored observation is then processed with the mSCID method by performing a cross-correlation on the full precursor length, resulting in super-resolved relative TOA adjustments. The adjusted time event and decoded subscriber information (if available) is then backhauled to the central processing site for association with other observations corresponding to the same MS. The location is then determined via TDOA multilateration techniques.

Since the Barker code is used for detection and message framing; as with any code matched detector, a static or dynamic threshold must be determined to give a desirable probability of intercept (POI). However, this is not always ideal as the probability of false alarms ( $P_{FA}$ ) may be excessive. This would then degrade resource efficiency, whether it occurs in the acquisition or decoding blocks of the listening station, or in the inter-network communications. It may be noted that the precursor has a strong localized 5 kHz energy component (i.e. 30 bits of dotting) that is primarily used for clock synchronization, but can also be used for detection. Typical base station hardware will use a narrowband filter centered at 5 kHz (or an associated harmonic if a  $N$ -law nonlinear process is used) followed by a peak log detection circuit. This parallel detection process

which utilizes both the dotting and Barker sequence is ideal in that it also provides framing/synchronization for NRZ data recovery if external interfaces to the wireless carrier's BS equipment (or MSC equipment) are unavailable for the deployed location technology. However, caution must be observed when implementing this process. For example, if the parallel detection is performed in software, it would be desirable to perform the narrow bandpass filtering at the desired spectral tone to minimize false triggers from out-of-band interferers and noise, which can easily be done with a simple biquadratic digital filter. However, to have such a narrow passband implies that the filter will have a characteristically long steady state response. Thus, by the time the narrowband filter output exceeds an assigned threshold indicating a possible RECC message, the Barker matched filter output may not correspond (i.e. a parallel implementation). Furthermore, the narrowband filter will have a forced response which can falsely indicate the presence of the 5 kHz dotting sequence, i.e. transient inputs into the digital filter can produce significant oscillations at the pole frequency.

Utilizing the exact CGSA of Telus Mobility for Calgary, Alberta, Klukas was able to ascertain through computer simulations, that the accuracy requirements of the FCC ruling are achievable when measurement subsets were restricted for an HDOP  $\leq 2$ . This was true for 73% of the CGSA of Calgary, resulting in 139 m *DMRS*. Without the geometrical restriction, the simulated accuracy was 344 m *DMRS*.

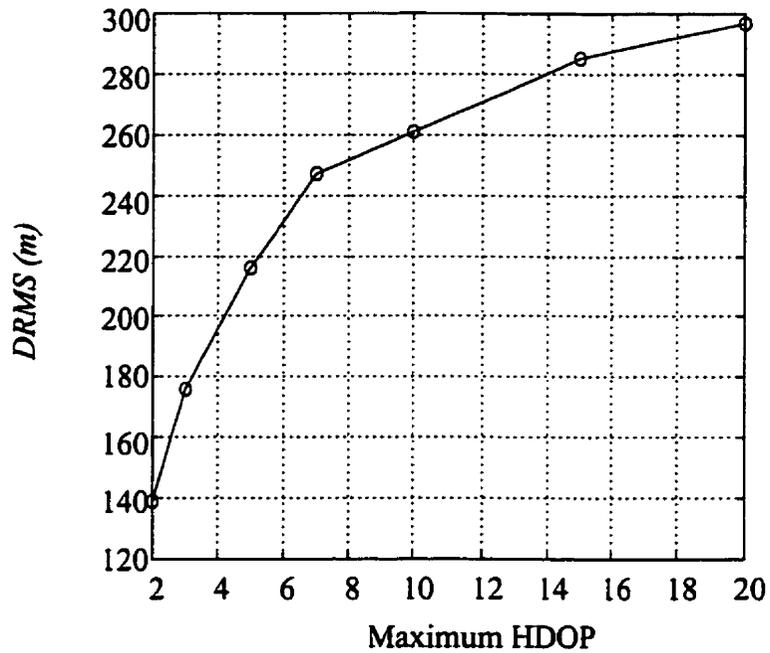


Figure 3.11. Simulated horizontal position accuracy for given HDOP [58].

Preliminary field trials were then conducted in Calgary, where Cell-Loc's prototype LS equipment (Cellocate) was deployed in four Telus Mobility cell sites. Test locations at known coordinates (obtained via DGPS with carrier phase smoothing) were chosen within the square test bed region, which covers approximately  $6.25 \text{ km}^2$ . Static measurement results were presented for three locations, which were conducted over two separate days to investigate repeatability. Results for two of the locations are given in Table 3.5.

Table 3.5 Static Data Precision and Accuracy Measurements [59]

Parameter	Location 1		Location 2	
	1.3		1.2	
HDOP				
Date (dd/mm/yy)	03/10/96	24/10/96	03/10/96	24/10/96
HP (m)	130	223	186	180
DRMS (m)	166	226	279	288

The other two-dimensional error measure given in Table 3.5 is the horizontal precision (HP), which is nearly identical to *DMRS*. The difference between the two measures is the value used for the sample mean. Thus, the error measures of [59] are given by

$$HP = \sqrt{\sigma_x^2 + \sigma_y^2} \quad \text{and} \quad DRMS = \sqrt{\sigma_x^2 + \sigma_y^2}, \quad \text{where} \quad m_x = \sum_{i=1}^N x_i / N \quad \text{and}$$

$$\sigma_x^2 = \sum_{i=1}^N (x_i - m_x)^2 / (N - 1) \quad \text{are the East (or } x) \text{ sample mean and variance obtained from}$$

the measured data, respectively. The North (or  $y$ ) components are obtained in a similar manner. The sample mean used in the *DRMS* error measure is the DGPS two-

dimensional coordinates of the pseudo phone, i.e.  $\sigma_x^2 = \sum_{i=1}^N (x_i - x_{DGPS})^2 / (N - 1)$  and

$$\sigma_y^2 = \sum_{i=1}^N (y_i - y_{DGPS})^2 / (N - 1).$$

One may note that the *DRMS* error measure is larger than the HP values. This is due to non-optimal biases being used in the multilateration algorithm, where the biases are attempting to account for the net lags through the BS RF front end (including antennas and cabling) and the Cellocate RF/IF receiver chain. This is evident from the results obtained over two separate days, and can be improved by more stringent group delay requirements imposed on the LS RF/IF receiver design.

Although the Cellocate system has demonstrated promising potential, it should be noted that the RECC transmissions are a single event and may not provide the level of confidence required by the FCC ruling. Therefore, multiple audits of the handset would alleviate this problem but not totally eliminate it.

There have been numerous discussions on the feature of subscriber location on inherent control channel signaling, where many individuals have expressed the opinion that excessive non-autonomous registrations would overload the cellular network and potentially tie up the RECC, resulting in network degradation and subscriber complaints. Kaufman [61] has recently quantified the timing and throughput of the RECC but has shown some misconceptions regarding the standards outlined in EIA/TIA-553. The RECC utilizes an access protocol that is a variant of carrier sense multiple access with collision detection (CSMA/CD). The RECC channel status is detected by the base station and broadcast over the FOCC on every 11<sup>th</sup> bit of the message stream which is designated as the busy/idle (B/I) bit.

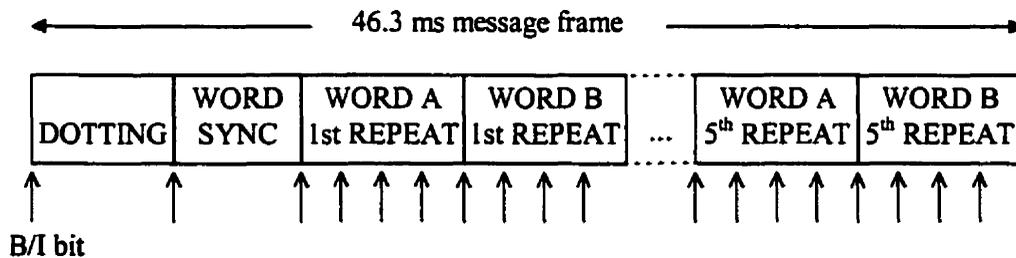


Figure 3.12. Base Station - to - Mobile Station (FOCC) message format.

When the subscriber initiates an access attempt the MS checks the B/I bit on the FOCC to see if the channel is in use. If the RECC is idle then the MS powers the carrier up to the designated level outlined in the FOCC global network messages and begins message transmission within 2 ms; i.e. carrier power and frequency stability must be achieved within 2 ms. Once transmission commences, a timer is started by the MS to monitor for

premature B/I bit transitions which would indicate if a collision has occurred from another MS attempting to gain access at nearly the same instant.

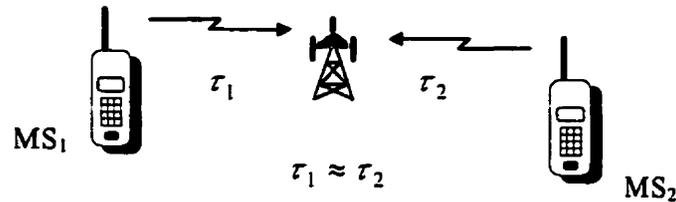


Figure 3.13. RECC collision.

If the B/I bit changes from idle to busy before the 56<sup>th</sup> bit of the message is transmitted then the MS treats this as a collision and halts transmission. After halting transmission, the MS will wait a random backoff time which is uniformly distributed between [0, 200 ms] before attempting another seizure attempt, again checking the FOCC B/I bits.

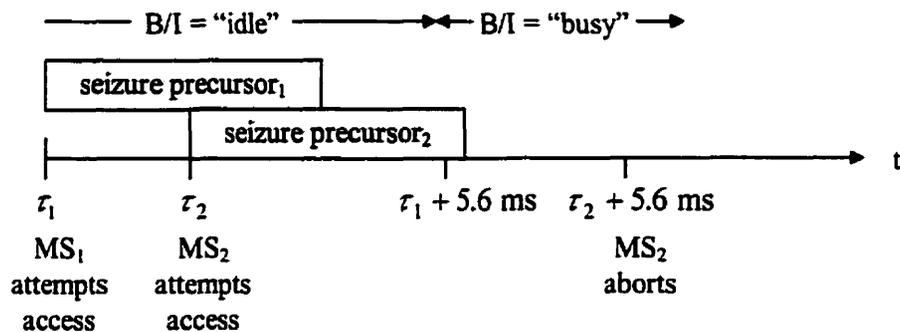


Figure 3.14. RECC collision occurring before 56 bits are transmitted.

If the MS had not observed a B/I transition before the 56<sup>th</sup> bit is sent it would then continue monitoring for a B/I transition until the 104<sup>th</sup> bit was sent. If by this time a B/I transition from idle to busy has not occurred then the MS assumes that a collision or fade has occurred and follows the same backoff procedure before attempting access again. It should be noted that the BS may let the MS time out rather than acknowledge the access attempt, especially for originations occurring when voice channels are unavailable.

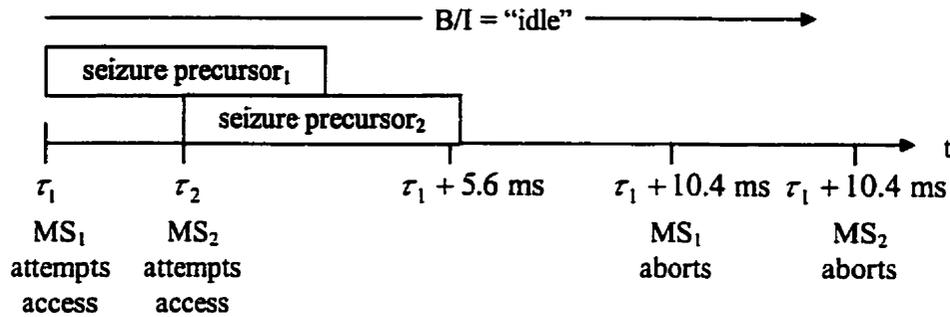


Figure 3.15. Failed RECC access attempt, determined after 104 bits.

Due to the fact that the maximum number of words allowed in a RECC message is six, with each word repeated five times, one can easily perform the following calculation:

$$\begin{array}{r}
 6 \text{ words} \\
 \times 5 \text{ repeats} \\
 \times 48 \text{ bits per word} \\
 \hline
 1440 \text{ bits} \\
 \times 100 \mu\text{s per bit} \\
 \hline
 144 \text{ ms}
 \end{array}$$

plus 4.8 ms for the precursor, as well as up to 2 ms for MS carrier settling time and an additional 25 ms of unmodulated carrier added to the end of the RECC message. This results in a total time of 175.8 ms, and places a conservative lower upper bound of 5 registrations per second on the RECC.

The BS must change the B/I status to busy between 0.8 ms and 2.9 ms after reception of the last bit of the MS's precursor. Now Kaufman argues that the 10.4 ms (i.e. 104 bits) window is too long to decide if the RECC access attempt should be aborted since the precursor is only 4.8 ms in length and the maximum B/I bit transition period is 2.9 ms after the last bit of the precursor is received. This gives  $4.8 \text{ ms} + 2.9 \text{ ms} = 7.7 \text{ ms}$ , while the TIA-553 standard requires the MS to wait an additional 2.7 ms before deciding that a RECC collision occurred. However, the MS is only able to discern the overhead network messages and B/I bits if it has synchronized to the FOCC message frame. If one assumes that every registration occurring from a MS must initially obtain

synchronization, and recalling that the FOCC message words are repeated 5 times to combat consecutive error hits incurred by the fading channel. The mobile station then performs three out of five majority voting on the B/I bits giving a time of  $4.8 \text{ ms} + 5.5 \text{ ms} = 10.3 \text{ ms}$ . This ensures that the MS has a reliable indication of the RECC idle status. Even if three consecutive B/I bits are accumulated with no discrepancies, implying that further B/I bit accumulation is not required, this places a  $4.8 \text{ ms} + 3.3 \text{ ms} = 8.1 \text{ ms}$  limit on the observation window. Thus, the timer constraints imposed in the EIA/TIA standards are sufficient and necessary.

### 3.5 Subscriber Identification

Although the interception and TOA determination of the air-interface signaling is instrumental to the location technology, identification of the MS is necessary to differentiate the desired subscriber from the multiple users. The FOCC is time multiplexed with subscriber and network information, and is interlaced with two message streams for "A" phones and "B" phones. The A and B streams on the FOCC should not be confused with the two distinct wireless service providers, i.e. the A side (or non-wireline side) and the B side (or wireline side). The A and B streams of the FOCC correspond to the least significant bit (LSB) of the subscriber's encoded  $\text{MIN}_1$ . Hence, phones that have the LSB of  $\text{MIN}_1$  equal to "0" and "1" are placed by the network (i.e. BS) onto the A stream and B stream, respectively.

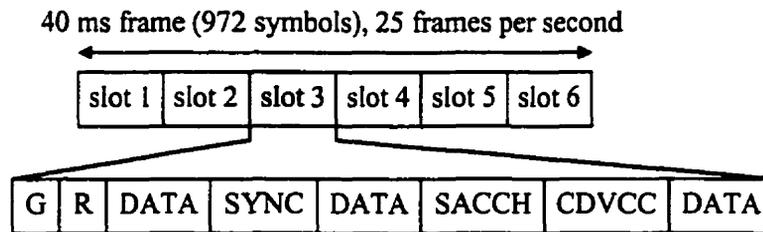
As previously outlined, all wideband data messages in the AMPS air interface standard are linearly block encoded and temporally repeated to combat burst errors induced by fading, i.e. bit-by-bit three out of five majority voting. The shortened (63,51) Bose-Chaudhuri-Hocquenghem (BCH) code used in the wideband data encoding is capable of correcting up to two bit errors. The original AMPS system was set up to disregard data messages that were corrupted by more than one bit error, resulting in the retransmission of the MS RECC message. Thus, any network-centric location

technology that resides independent from the BS equipment must try to extract appropriate data fields on all access attempts, including those rejected by the BS. The miss rate of the RECC messages should be in the range of  $10^{-3}$  for an SIR of 15 dB, and the falsing rate (incorrect data interpretation) should be less than  $10^{-7}$  for a given message. However, the falsing rate is based on non-coherent FSK where the instantaneous carrier envelope is 15 dB above the noise level. When the system is subject to Rayleigh fading, where the average carrier envelope is 15 dB above the noise level then the probability of bit error becomes approximately 3% which is extremely poor and is an important issue for any network-centric location technology to resolve for proper subscriber identification.

Although the word block is repeated five times to combat burst errors incurred on the multipath channel, the framing must be reliably obtained from the bit synchronization and the word sync, i.e. the 11 bit Barker code. Subsequently, if the framing is a single bit off then all word blocks will be in error. The 11 bit Barker code provides excellent cross-correlation properties, however, for low SNR signals the threshold for its matched filter output must be reduced in order to achieve a reasonable acquisition rate and framing rate. This reduced threshold will then increase the false alarm rate and indicate incorrect word block frames. The low SNR conditions will also introduce bit errors, while burst errors will occur due to cycle slips on the demodulated output of the PLL (i.e. FM threshold or PLL threshold level), resulting in corrupt subscriber data (e.g. MIN, ESN, Called Party). This may be a significant issue in E911 applications as any errors incurred in the extracted Called Party field may bypass the location determination process. Pattern recognition may be applied on the subscriber data to account for minor digit errors, e.g. "211" ↔ "911", but multiple digit errors cannot be corrected.

### 3.6 IS-54-B Time-of-Arrival Processing

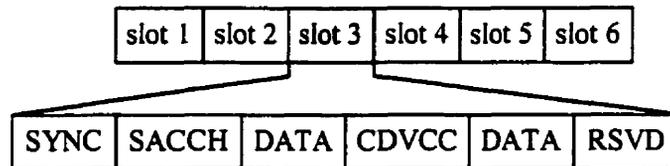
In order for the mobile station to gain network access on the RDTCs, whether from call originations, page responses, or handoffs, the mobile station must have a proper time alignment so that its burst messages arrive at the base station receiver in the proper time relationship with regard to other burst periods (BP).



G - Guard Time  
R - Ramp Time

SACCH - Slow Associated Control Channel  
CDVCC - Coded Digital Verification Color

Figure 3.16. Mobile Station - to - Base Station (RDTC) slot format.



RSVD - Reserved for future definitions.  
Defaulted to encoded zeros.

Figure 3.17. Base Station - to - Mobile Station (FDTC) slot format.

During network access (i.e. initial RDTc assignments), or when initiated by the base station during an established call (e.g. handoffs), the normal supervision and control messages shown in Fig. 3.16 are replaced by the shortened burst.

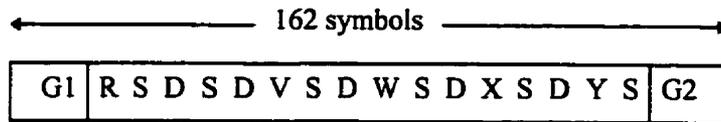


Figure 3.18. Shortened Burst format.

Where G1 is a 3 symbol guard time, R is a 3 symbol ramp time, S is the 14 symbol sync word, D is the 6 symbol CDVCC, G2 is a 22 symbol guard time, and {V, W, X, Y} are  $\pi/4$  - DQPSK precoded zero bits of varying length.

The mobile station will continuously transmit the shortened burst at a default offset period until it receives a time alignment message from the base station, or until the access timer of the mobile station is exceeded (i.e. five seconds). If the access timer has expired then the MS assumes that the assigned channel has been dropped due to fading and halts transmission. The MS will then scan all primary control channels and attempt to reinitiate a network link. It may be noted that the successive transmission of the shortened burst allows averaging, which may reduce measurement errors and other blunders, thus improving the confidence level of the position estimate.

During this synchronization process, the base station is able to determine the time alignment of the mobile station after detecting any two sync words of the shortened burst, as the sync words are at known symbol separations. However, errors can arise in the time alignment when the burst overlaps into an adjacent BP, but this problem may be quickly corrected because the individual time slots are assigned unique sync words. These 14 symbol sync words should not be confused with the Barker code used in the analog control channels, and are achieved by the following phase changes.

Table 3.6 Time Slot Synchronization Sequences (normalized by  $\pi/4$ )

Slot	Synchronization Sequence													
1	-1	-1	-1	3	1	3	-3	3	-3	-1	3	1	-1	-1
2	-1	-1	-1	3	-3	3	1	3	1	-1	3	-3	-1	-1
3	-3	1	3	-3	-3	-1	1	-3	-3	1	1	1	-3	1
4	1	-3	3	1	1	-1	-3	1	1	-3	-3	-3	1	-3
5	1	3	1	-3	-3	-1	1	-1	1	-3	-3	3	1	3
6	-3	3	-3	1	1	-1	-3	-1	-3	1	1	3	-3	3

The base station utilizes the shortened burst to identify the individual time slots due to its unique cross-correlation properties, thus, making these known sequences ideal for determining the MS's location. One may observe that several variants of a reference correlation sequence (or code) exist for the shortened burst:

- i) initial 14 symbol sync word designated for the time slot;
- ii) concatenated code consisting of the 14 symbol sync word and the 6 symbol CDVCC;
- iii) varying lengths of the concatenated 14 symbol sync word, 6 symbol CDVCC, and precoded zero bits;
- iv) the whole shortened burst.

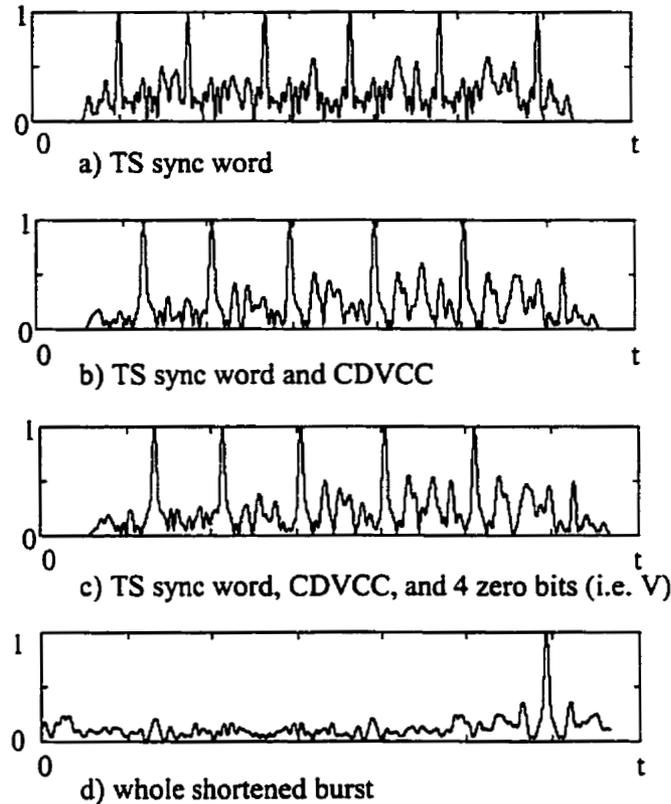


Figure 3.19. Normalized cross correlation sequences for time slot 3 and CDVCC 1 (noiseless case).

One may utilize the longer potential codes to achieve increased processing gains and longer time-bandwidth products, however, it can be observed that the increased sequence lengths do not necessarily imply TOA improvement as the cross-correlation properties become sub-optimal and the self-generated correlation sidelobes can increase the bias and variance in the TOA estimates. Thus, it was decided to use the 14 symbol sync word of the appropriate time slot as the reference sequence. This code has the benefit that the sequences can easily be stored in onboard memory devices, since knowledge of the CDVCC is not required. Since six sync words are employed per shortened burst, a small ensemble analysis may be performed per BP to minimize the multipath channel effects, especially since NADC *RMS* delay measurements of  $2 - 3\mu\text{s}$

were observed in urban environments [62, 63] and can easily introduce errors. An additional benefit of the chosen reference sequence is that positioning can also be performed on normal digital traffic channel bursts, which occur more frequently than the synchronization process. TOA processing on a RDTC also minimizes the issue of inter-network communication latency, which occurs when relying solely on the shortened burst. Furthermore, averaging position estimates obtained from multiple transmissions of the shortened burst may only be reserved for subscriber initiated location services as long periods of muted voice may result in subscriber complaints. In fact, AGT Mobility had turned off the shortened burst feature on its digital network due to numerous complaints of long muted periods during normal handoff operations of digital voice channels [64]. Other existing digital systems such as GSM have implemented an adaptive method in their time slot synchronization to minimize long periods of muted speech.

As can be noticed from Table 3.3, the operating power levels for the digital mode can be significantly lower than the analog mode. This makes interception at distant listening stations extremely difficult when utilizing the time slot synchronization sequence. If acquisition were performed solely on the time slot sequence then the detection threshold of the matched filter would have to be reduced. Although the POI would be slightly increased, the  $P_{FA}$  would become excessive and degrade the overall system performance. An approach to alleviate this problem is to exploit the organization of the RDTC and FDTC frames. The uplink and downlink frames are offset in time by a nominal 207 symbol periods to minimize hardware requirements in the handset. Thus, time slot 1 of frame  $N$  of the FDTC occurs 207 symbols after time slot 1 of frame  $N$  of the RDTC.

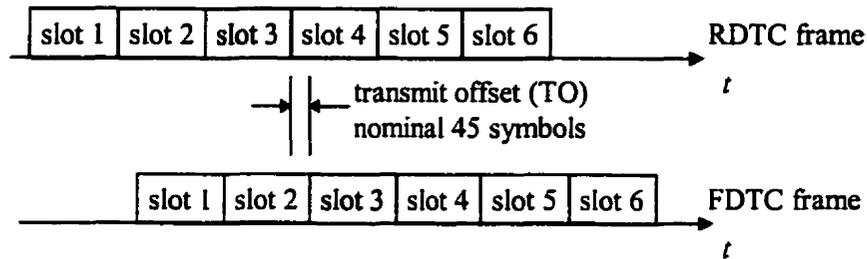


Figure 3.20. Standard offset for digital traffic channels with no timing advance.

A 5 bit absolute time alignment (TA) offset field exists in the NADC system, which corresponds to the standard offset reference position. This TA field allows the BS to advance or retard the handset's BP in units of half symbol periods, i.e.,

$$TO = \left[ 45 \pm \frac{TA}{2} \right] T_{symbol} \pm \frac{T_{symbol}}{4}. \quad (3.6)$$

Since the network maintains this standard offset between the FDTC and the RDTC, it is possible to utilize this relation to avoid time slot sequence acquisition at the remote sites, and possibly even at the serving cell, where one may extract the required slot/frame timing from the FDTC at the serving cell. Since the location technology is expected to be co-located with the BS equipment, then the FDTC signal levels can easily be designed for in the receiver's RF front end. Even cell sites that have the BS equipment separated by several building floors from the RF antennas will pose no difficulties, i.e. levels obtained from RF bay leakage, cable leakage, or building loss should be adequate to determine the timing relationship. Therefore, the cross-correlation of the time slot sequence is performed on the FDTC, with the correlation lobe referenced to GPS time, and routed to the other listening stations via existing DS1 links. The remote LS units can then remove the frame modularity (i.e. 40 ms frame and the associated TO) of the received reference time and the present GPS time at each individual unit. Thus, the observation window is easily synchronized to the desired time slot for the TOA

measurement process. Where the synchronized observation window is used for the cross-correlation of either the time slot sequence, or one of the other possible concatenated codes if the shortened burst is used.

It appears that no further difficulties exist for the TOA acquisition process, however, although we know when the MS's BP occurs, it is still unknown whether the BP is utilized by the MS at that instant. Recall that the MS is allowed to turn off its transmitter when operating in the  $DT_x$  mode, or the MS may be tuned to a different carrier frequency when performing channel quality measurements (CQM). Thus, a BP detector is required to ensure that channel noise is not wastefully processed. A worse condition can occur when a cochannel burst is mistakenly processed in the position estimate (which is more difficult to detect). One possible method of detecting the activity of the designated time slot is to utilize a matched filter designed for the TS sync word. However, this approach has limited applicability due to the lower SNRs involved, as was previously discussed. Another approach is to utilize nonlinear processes that exploit the spectral correlation (i.e. cyclostationarity) of the signal.

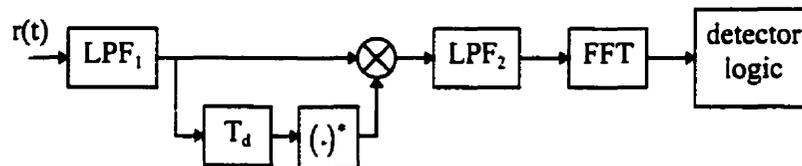


Figure 3.21. General receiver for BP activity detection.

These architectures are typically used for symbol timing recovery and residual frequency estimation/correction [65, 66], however, it is also possible to utilize these designs for signal detection [67]. Such nonlinear architectures produce spectral lines that exist for certain integer ratios of the fundamental symbol period, i.e.  $f \in \frac{k}{T_{symbol}}$ . Thus, Fig. 3.21 provides a spectral line at the symbol rate, indicating the presence or absence of the SOI.

Of course one can realize several variants of the above architecture or of other designs that provide the same harmonic component(s).

Briefly examining the conjugate delay - product architecture of Fig. 3.21, the magnitude of the desired spectral line can be compared with an appropriate threshold based on the receiver spectral noise estimate, which would also include algorithm self-noise. If for example, a RRC matched filter is used for  $LPF_1$  and a simple recursive running sum (RRS) filter is used for  $LPF_2$ , the following results are obtained. Other parameters include a sample rate of  $f_s = 32/T_{symbol}$ , a residual frequency error of 96 Hz, and an initial signal conversion level of 5 bits of a 12-bit analog-to-digital converter (ADC), which is assumed to correspond to a 20 dB SNR.

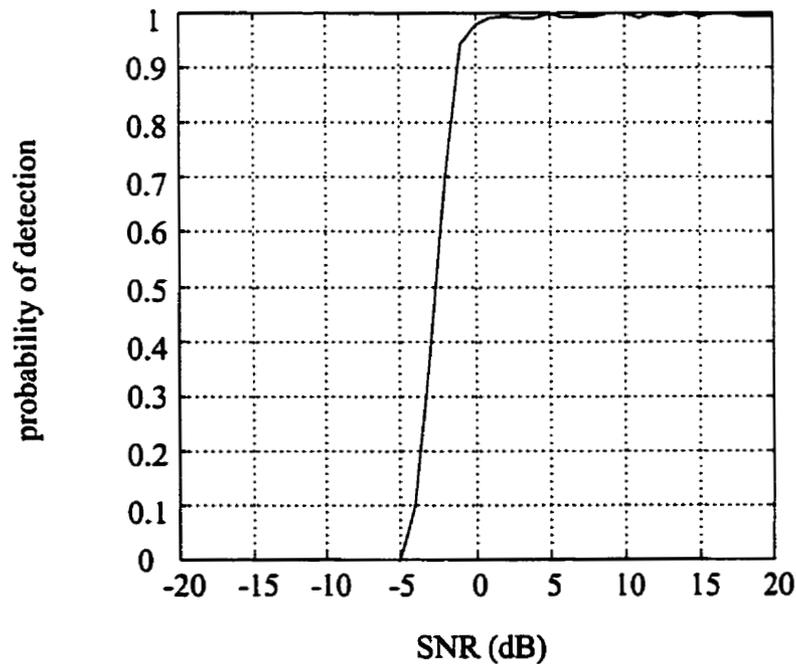


Figure 3.22. BP architecture operating characteristics for NADC SOI.

Since the sample rate is 32 times the symbol frequency, it was expected that the SNR performance would degrade near  $-10 \log_{10}(32) = -15$  dB, yet the performance degrades

sooner due to the low conversion levels at the ADC. This may be improved if one adds variable gain in the front-end receiver, allowing the full scale dynamic range (FSDR) of the ADC to be utilized. However, caution must be exercised if using this method to ensure that the receiver operates in its linear region.

## **Chapter 4: NADC Geolocation**

### **4.1 Digital Cellular Radio Positioning**

Propagation modeling of the mobile radio environment can at times be confusing because several different models are available, and each one may be appropriate under certain constraints and assumptions. As mentioned in Chapter Two, most researchers in wireless location at the University of Calgary have used Hashemi's SURP model for their simulations, however, this routine can become computationally intensive and time consuming if numerous trial runs are performed with only slightly varying parameter conditions. There are some other classical propagation models that can be used such as the Okumura-Hata model [68], the Carey model [69], and the Walfisch-Ikegami model [70] that were also derived from outdoor measurements in varying multipath environments. There are simpler models such as the plane earth propagation model that was chosen for the IS-54-B positioning simulations conducted in this thesis due to the fact that the computational operations required were minimal and the resultant SNR was near to other model predictions for given baselines. The use of the plane earth propagation model allowed numerous trial runs to be conducted in a reasonable processing time as the super-resolution method is computationally intensive. The simulations assumed that the mobile station was stationary during its burst period, an assumption which may be questionable in regards to "real world" applicability. However, even if the MS was traveling at a high rate of speed, such as 150 km/hr (41.7 m/s), the physical distance traveled is negligible as a single time slot period is approximately 6.7 ms in duration. It should also be noted that if the positioning is applied for emergency situations then most 911 callers will be stationary unless a passing good-hearted Samaritan happens to call in the accident.

## 4.2 Path Loss Models

A simplified path loss model is based on the free-space propagation model

$$\frac{P_R}{P_T} = G_T G_R \left( \frac{\lambda}{4\pi d} \right)^n, \quad (4.1)$$

where  $d$  is the transmit and receive antenna baseline,  $\lambda$  is the common RF wavelength,  $n = 2$  is the propagation decay constant operating in free space,  $G_T$  and  $G_R$  are the antenna gains for the transmitter and receiver, respectively. To make (4.1) independent of the antenna gains we can assume that the transmission is between two isotropic antennas of unity gain, thus the path loss can be written as:

$$\begin{aligned} L_p &= \left( \frac{4\pi d}{\lambda} \right)^2 \\ L_p(dB) &= 20 \log_{10} \left( \frac{4\pi d}{\lambda} \right) \\ L_p(dB) &= 20 \log_{10} \left( \frac{4\pi}{c} \right) + 20 \log_{10}(f) + 20 \log_{10}(d), \end{aligned} \quad (4.2)$$

where  $c$  is the velocity of light in free space, and  $f$  is the carrier frequency.

When the propagation is over a conducting surface, i.e. plane earth model, then the propagation loss between the two isotropic antennas is given by

$$L_p = \left( \frac{d^2}{h_T h_R} \right)^2, \quad (4.3)$$

where  $h_T$  and  $h_R$  are the antenna heights of the transmitter and receiver, respectively. It can be noticed that the baseline loss is now proportional to the fourth power of the baseline  $d$ . Typically, the gains associated with the antenna heights can be neglected due to coupling losses, cabling losses, etc. Thus, the simplified propagation model becomes

$$L_p(dB) = 20 \log_{10} \left( \frac{4\pi}{c} \right) + 20 \log_{10}(f) + 40 \log_{10}(d). \quad (4.4)$$

Okumura [71] has derived a graphical technique based on numerous measurements collected in the Tokyo region. Masaharu Hata then obtained analytical expressions from this data to model propagation in three urban environments. The first is for small-to-medium cities which is termed as urban, and the other two are for large cities which are frequency parameterized. Hata also derived correction factors for suburban and rural environments. The model is given by

$$L_u(dB) = 69.55 + 26.16 \log_{10}(f_c) - 13.82 \log_{10}(h_{br}) - a(h_{ms}) + [44.9 - 6.55 \log_{10}(h_{br})] \log_{10}(d), \quad (4.5)$$

where  $L_u$  is the urban propagation loss in dB,  $f_c$  is the carrier frequency in MHz,  $h_{br}$  and  $h_{ms}$  are the antenna elevations in meters for the BS and MS respectively,  $d$  is the baseline formed by the BS and MS in km, and  $a(h_{ms})$  is a correction factor for the severity of the multipath mobile radio environment.

The correction factor for small to medium cities may be computed using:

$$a(h_{ms}) = [1.1 \log_{10}(f_c) - 0.7] h_{ms} - 1.56 \log_{10}(f_c) - 0.8. \quad (4.6)$$

As previously mentioned, the correction factor for large cities is frequency parameterized, where

$$a(h_{ms}) = \begin{cases} 8.29 \log_{10}^2(1.54 h_{ms}) - 1.1, & f_c \leq 200 \text{MHz} \\ 3.2 \log_{10}^2(11.75 h_{ms}) - 4.97, & f_c \geq 400 \text{MHz} . \end{cases} \quad (4.7)$$

Hata has also derived additional correction factors for the above analytic expressions for less dense environments. These are given by:

$$\text{Suburban correction } L_s(dB) = L_u - 2 \log_{10}^2\left(\frac{f_c}{28}\right) - 5.4 \quad (4.8)$$

$$\text{Rural correction } L_r(dB) = L_u - 4.78 \log_{10}^2(f_c) + 18.33 \log_{10}(f_c) - 40.94. \quad (4.9)$$

The above analytical expressions were based on measurements obtained by Okumura so the constraints for the propagation model are:

$$150\text{MHz} \leq f_c \leq 1500\text{MHz}, 30\text{m} \leq h_{bs} \leq 200\text{m}, 1\text{m} \leq h_{ms} \leq 10\text{m}, \text{ and } 1\text{km} \leq d \leq 20\text{km}.$$

If one were to compare the baseline dependent terms for the urban propagation model (4.2) and the simplified propagation loss model (4.1), one would obtain the following:

$$\begin{aligned} [44.9 - 6.55 \log_{10}(h_{bs})] \log_{10}(d) &\equiv 10n \log_{10}(d) \\ n &\equiv \frac{1}{10} [44.9 - 6.55 \log_{10}(h_{bs})]. \end{aligned} \quad (4.10)$$

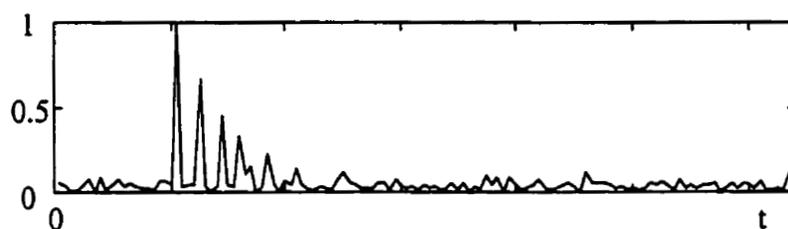
One may observe, that if the model limitations for the BS antenna elevation were to be applied to (4.8) then the propagation decay constant would become bounded between  $2.98 \leq n \leq 3.52$ . From this result it can be surmised that setting  $n = 4$  (i.e. an  $h_{bs} < 30\text{m}$ ) for the baseline term in the simplified propagation loss model is a valid assumption in the simulations for expected path loss.

The Walfisch-Ikegami model is useful for dense urban environments and is based on parameters such as building density and average height, and street widths as it is trying to account for urban canyon waveguiding effects by utilizing ray tracing. It has three main propagation loss factors:

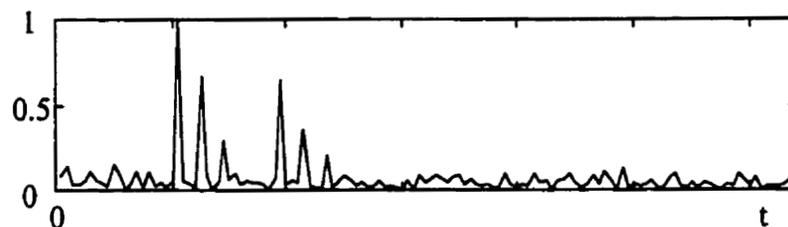
- i) free space loss,
- ii) diffraction loss, and
- iii) obstruction loss.

This model is far better suited for microcell simulations and was not considered in this analysis as a mobile radio channel corresponding to a typical Canadian wireless cell was considered rather than cells structured for dense subscriber bases.

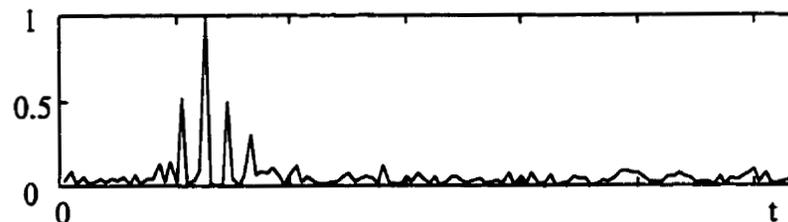
Although the propagation model used in the simulations has been set, there is still the issue of the channel delay spread which determines the resolution of the LOS component in the signal reception. Typically for urban environments the *RMS* channel delay spread is around 2-3  $\mu\text{s}$ . There are essentially three CIR types for the mobile radio environment, the first of which is the “typical” response in which the multipath components trail the LOS component with decreasing amplitude as the components increase in differential delay. The second type is called disjoint because there exists a distinct gap between the first cluster with the LOS component and the secondary cluster arrival. The last CIR type is the one where the direct path is either attenuated or constructive interference occurs on the multipath components.



a) typical response



b) disjoint response



c) attenuated response

Figure 4.1. Illustration of typical normalized CIR delay profiles.

### 4.3 TOA Multilateration

In past research, Turin *et al.* [72] examined a “true” least squares formulation for a simulated automatic vehicle monitoring (AVM) system for narrowband and wideband mobile radio classes, where all fixed sensor measurements were used with equal weights in the solution process.

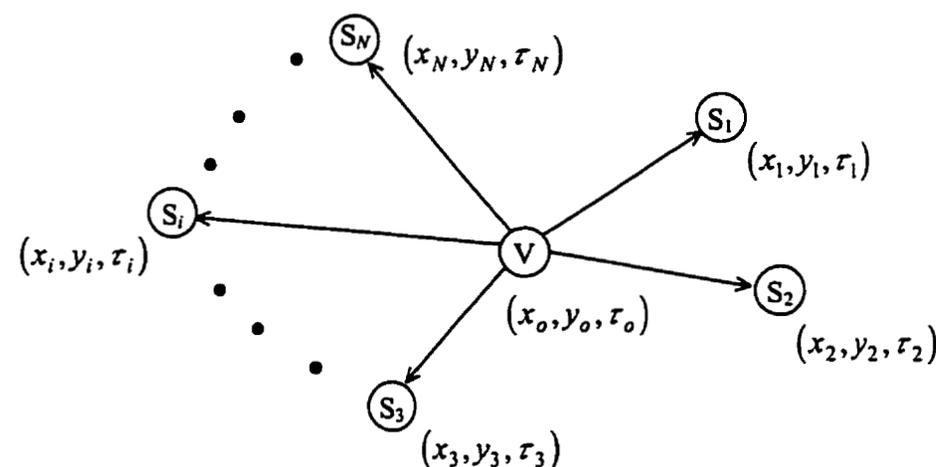


Figure 4.2. Geometry of AVM system.

The vehicle V, or in our case the mobile station, is located at coordinates  $(x_o, y_o)$  and transmits either a burst signal or continuous signal at time  $\tau_o$  which typically is unknown, but may be known within a quantized resolution for digital systems (e.g. IS-54-B, IS-136 TDMA, and IS-95 CDMA systems). The  $N$  listening stations or sensors  $\{S_i\}_1^N$  are located at known coordinates  $(x_i, y_i)_1^N$  and receive the transmitted signal at a time estimate  $\tau_i$ , which of course is corrupted by the multipath channel. The time estimates are then referenced to a common master clock. An objective function can now be formulated for two-dimensional positioning:

$$f_i(x, y, \tau) = c(\tau_i - \tau) - \sqrt{(x_i - x)^2 + (y_i - y)^2} \quad \forall i = 1, \dots, N, \quad (4.11)$$

where  $c$  is the velocity of light,  $(x, y)$  are the estimated coordinates of the vehicle and  $\tau$  is the estimated time of the transmission (with measurement errors and multipath errors).

An estimate  $(\hat{x}, \hat{y}, \hat{\tau})$  of  $(x_o, y_o, \tau_o)$  is then used in a weighted least-squares minimization of the function

$$F(x, y, \tau) = \sum_{i=1}^N \alpha_i^2 f_i^2(x, y, \tau), \quad (4.12)$$

where  $\alpha_i$  is the designated weight for the  $i^{\text{th}}$  signal reception. The time of transmission estimate can be neglected once a convergent solution exists since one is only interested in the location coordinates.

Now if the nonlinear function  $f_i(x)$  is linearized, and the higher order detail of the error representation is truncated, one may obtain the following:

$$\begin{aligned} f_i'(x, y, \tau) &= -c\partial\tau - \frac{[-2(x_i - x)\partial x - 2(y_i - y)\partial y]}{2\sqrt{(x_i - x)^2 + (y_i - y)^2}} \\ &= -c\partial\tau + \frac{(x_i - x)\partial x}{\sqrt{(x_i - x)^2 + (y_i - y)^2}} + \frac{(y_i - y)\partial y}{\sqrt{(x_i - x)^2 + (y_i - y)^2}} \end{aligned} \quad (4.13)$$

$$f_i(x, y, \tau) = f_i(\hat{x}_0, \hat{y}_0, \hat{\tau}_0) + \frac{(x_i - \hat{x}_0)\partial x}{r_i} + \frac{(y_i - \hat{y}_0)\partial y}{r_i} - c\partial\tau, \quad (4.14)$$

where

$$r_i = \sqrt{(x_i - \hat{x}_0)^2 + (y_i - \hat{y}_0)^2}. \quad (4.15)$$

Now if one examines discrete interval sizes, then (4.14) becomes

$$f_i(x, y, \tau) = f_i(\hat{x}_0, \hat{y}_0, \hat{\tau}_0) + \Delta x_i(x - \hat{x}_0) + \Delta y_i(y - \hat{y}_0) - c(\tau - \hat{\tau}_0), \quad (4.16)$$

where

$$\Delta x_i = \frac{(x_i - \hat{x}_0)}{r_i}, \text{ and } \Delta y_i = \frac{(y_i - \hat{y}_0)}{r_i}. \quad (4.17)$$

One may then substitute  $h, k, u$  into (4.16) to obtain the following:

$$f_i(x, y, \tau) = f_i(\hat{x}_0, \hat{y}_0, \hat{\tau}_0) + \Delta x_i h + \Delta y_i k - cu, \quad (4.18)$$

where

$$h = (x - \hat{x}_0), k = (y - \hat{y}_0), u = (\tau - \hat{\tau}_0). \quad (4.19)$$

This after simplification results in

$$\begin{aligned} F(x, y, \tau) &\cong \tilde{F}(x, y, \tau) \\ &= \sum_{i=1}^N \alpha_i^2 [f_i(\hat{x}_0, \hat{y}_0, \hat{\tau}_0) + \Delta x_i h + \Delta y_i k - cu]^2. \end{aligned} \quad (4.20)$$

The objective function (4.20) above, may now be minimized with respect to (4.19) such that

$$\frac{\partial \tilde{F}}{\partial h} = \frac{\partial \tilde{F}}{\partial k} = \frac{\partial \tilde{F}}{\partial u} = 0 \quad (4.21)$$

under the constraint

$$|h| + |k| + c|u| < \varepsilon, \quad (4.22)$$

where  $\varepsilon$  is a prescribed error tolerance for terminating the iterative process.

Therefore, one obtains:

$$\begin{aligned} \frac{\partial \tilde{F}}{\partial h} &= \sum_{i=1}^N 2\alpha_i^2 [f_i(\hat{x}_0, \hat{y}_0, \hat{\tau}_0) + \Delta x_i h + \Delta y_i k - cu] \Delta x_i = 0 \\ \frac{\partial \tilde{F}}{\partial k} &= \sum_{i=1}^N 2\alpha_i^2 [f_i(\hat{x}_0, \hat{y}_0, \hat{\tau}_0) + \Delta x_i h + \Delta y_i k - cu] \Delta y_i = 0 \\ \frac{\partial \tilde{F}}{\partial u} &= \sum_{i=1}^N 2\alpha_i^2 [f_i(\hat{x}_0, \hat{y}_0, \hat{\tau}_0) + \Delta x_i h + \Delta y_i k - cu] (-c) = 0. \end{aligned} \quad (4.23)$$

Now rewriting the above simultaneous equations in common vector notation,

i.e.  $\mathbf{Ax} = \mathbf{b}$ , yields:

$$\begin{aligned} \left( \sum_{i=1}^N \alpha_i^2 \Delta x_i^2 \right) h + \left( \sum_{i=1}^N \alpha_i^2 \Delta x_i \Delta y_i \right) k - \left( c \sum_{i=1}^N \alpha_i^2 \Delta x_i \right) u &= - \sum_{i=1}^N \alpha_i^2 \Delta x_i f_i(\hat{x}_0, \hat{y}_0, \hat{\tau}_0) \\ \left( \sum_{i=1}^N \alpha_i^2 \Delta x_i \Delta y_i \right) h + \left( \sum_{i=1}^N \alpha_i^2 \Delta y_i^2 \right) k - \left( c \sum_{i=1}^N \alpha_i^2 \Delta y_i \right) u &= - \sum_{i=1}^N \alpha_i^2 \Delta y_i f_i(\hat{x}_0, \hat{y}_0, \hat{\tau}_0) \\ - \left( c \sum_{i=1}^N \alpha_i^2 \Delta x_i \right) h - \left( c \sum_{i=1}^N \alpha_i^2 \Delta y_i \right) k + \left( c^2 \sum_{i=1}^N \alpha_i^2 \right) u &= c \sum_{i=1}^N \alpha_i^2 f_i(\hat{x}_0, \hat{y}_0, \hat{\tau}_0) \end{aligned} \quad (4.24)$$

$$\begin{bmatrix} \sum_{i=1}^N \alpha_i^2 \Delta x_i^2 & \sum_{i=1}^N \alpha_i^2 \Delta x_i \Delta y_i & -c \sum_{i=1}^N \alpha_i^2 \Delta x_i \\ \sum_{i=1}^N \alpha_i^2 \Delta x_i \Delta y_i & \sum_{i=1}^N \alpha_i^2 \Delta y_i^2 & -c \sum_{i=1}^N \alpha_i^2 \Delta y_i \\ \sum_{i=1}^N \alpha_i^2 \Delta x_i & \sum_{i=1}^N \alpha_i^2 \Delta y_i & -c \sum_{i=1}^N \alpha_i^2 \end{bmatrix} \begin{bmatrix} h \\ k \\ u \end{bmatrix} = - \begin{bmatrix} \sum_{i=1}^N \alpha_i^2 \Delta x_i f_i(\hat{x}_0, \hat{y}_0, \hat{\tau}_0) \\ \sum_{i=1}^N \alpha_i^2 \Delta y_i f_i(\hat{x}_0, \hat{y}_0, \hat{\tau}_0) \\ \sum_{i=1}^N \alpha_i^2 f_i(\hat{x}_0, \hat{y}_0, \hat{\tau}_0) \end{bmatrix} \quad (4.25)$$

Now by solving (4.25) with an initial estimate of the MS coordinates and time of transmission  $(x_0, y_0, \tau_0)$ , the solution set  $(h, k, u)$  obtained may then be checked against the error tolerance in (4.22). If the solution set fails the error tolerance then the process is repeated with the following updated estimates:

$$\hat{x}'_0 = \hat{x}_0 + h, \hat{y}'_0 = \hat{y}_0 + k, \hat{\tau}'_0 = \hat{\tau}_0 + u. \quad (4.26)$$

#### 4.4 Matrix Conditioning and Algorithm Stability

One may observe from (4.26) that the local minimum is obtained from the minimization of the consecutive step sizes in the iterative adjustments. If one were to recall the static optimization of a scalar valued function  $f(x)$ , where  $x$  is the scalar variable and it is desired that  $\hat{x} \in x$  minimize  $f(x)$ . One knows that a necessary condition for  $\hat{x}$  to be a local minimum of  $f(x)$  is that the derivative of  $f(x)$  evaluated at  $\hat{x}$  be equal to zero, i.e.,

$$\left. \frac{\partial f(x)}{\partial x} \right|_{x=\hat{x}} = 0. \quad (4.27)$$

Now the sufficient condition that  $\hat{x}$  be a local minimizer is that the second derivative of  $f(x)$  at  $\hat{x}$  be greater than zero, i.e.,

$$\left. \frac{\partial^2 f(x)}{\partial x^2} \right|_{x=\hat{x}} > 0. \quad (4.28)$$

Similarly for vector valued variables, if  $F(\mathbf{x})$  is a scalar function of a vector variable  $\mathbf{x}$  then the necessary condition for  $\hat{\mathbf{x}}$  to minimize  $F(\mathbf{x})$  is that the gradient vector  $\mathbf{F}(\mathbf{x})$  be zero for  $\mathbf{x} = \hat{\mathbf{x}}$ ,

where

$$\mathbf{x} = \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}, \quad \mathbf{F}_x = \begin{bmatrix} \frac{\partial F}{\partial x_1} \\ \vdots \\ \frac{\partial F}{\partial x_n} \end{bmatrix}, \quad \text{and} \quad \mathbf{F}_x|_{\mathbf{x}=\hat{\mathbf{x}}} = 0. \quad (4.29)$$

The sufficient condition is that the Hessian matrix  $\mathbf{F}_{xx}$  be positive definite,

where

$$\mathbf{F}_{xx} = \begin{bmatrix} \frac{\partial^2 F}{\partial x_1 \partial x_1} & \frac{\partial^2 F}{\partial x_1 \partial x_2} & \cdots & \frac{\partial^2 F}{\partial x_1 \partial x_n} \\ \frac{\partial^2 F}{\partial x_2 \partial x_1} & \frac{\partial^2 F}{\partial x_2 \partial x_2} & \cdots & \frac{\partial^2 F}{\partial x_2 \partial x_n} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{\partial^2 F}{\partial x_n \partial x_1} & \frac{\partial^2 F}{\partial x_n \partial x_2} & \cdots & \frac{\partial^2 F}{\partial x_n \partial x_n} \end{bmatrix}. \quad (4.30)$$

$$\therefore \mathbf{F}_{xx} = \begin{bmatrix} \sum_{i=1}^N 2\alpha_i^2 \Delta x_i^2 & \sum_{i=1}^N 2\alpha_i^2 \Delta x_i \Delta y_i & -c \sum_{i=1}^N 2\alpha_i^2 \Delta x_i \\ \sum_{i=1}^N 2\alpha_i^2 \Delta x_i \Delta y_i & \sum_{i=1}^N 2\alpha_i^2 \Delta y_i^2 & -c \sum_{i=1}^N 2\alpha_i^2 \Delta y_i \\ -c \sum_{i=1}^N 2\alpha_i^2 \Delta x_i & -c \sum_{i=1}^N 2\alpha_i^2 \Delta y_i & c^2 \sum_{i=1}^N 2\alpha_i^2 \end{bmatrix} \quad (4.31)$$

However, Turin's formulation [72] does not guarantee that the Hessian be positive definite as is shown in (4.31). This was indirectly suggested by Turin, that a gradient search technique be used to ensure convergence, although a unique global minimum is not guaranteed.

Now in the least squares formulation developed by Turin, an ill-conditioned matrix is produced where the symptoms of the ill-conditioning are the emergence of:

- i) small pivotal element used in the inversion process to solve  $\mathbf{Ax} = \mathbf{b}$  ;
- ii) large computed solution, i.e. a possible solution set of  $(x, y, \tau)$  being  $(\infty, \infty, -\infty)$  ;
- iii) large residual vector.

In Turin's method, there is the possibility of using iterative improvements of the approximate solution in order to circumnavigate the effects of the ill-conditioned formulation. One approach is to employ Hotelling's method. Typically, this method is used as a check of the accuracy of the matrix obtained by the selected inversion process. Let the matrix  $\mathbf{D}_0$  be the initial approximation of  $\mathbf{A}^{-1}$ , thus the product  $\mathbf{AD}_0$  will indicate the degree of inaccuracy between it and the unit matrix:

$$\mathbf{F}_0 = \mathbf{I} - \mathbf{AD}_0. \quad (4.32)$$

Thus, the elements of the inverse matrix,  $\mathbf{A}^{-1}$ , may be computed to as high an accuracy as desired (within machine precision of course) by utilizing the following iterative process. Let us form the following sequence of matrices:

$$\begin{aligned} \mathbf{D}_1 &= \mathbf{D}_0(\mathbf{I} + \mathbf{F}_0), & \mathbf{F}_1 &= \mathbf{I} - \mathbf{AD}_1 \\ \mathbf{D}_2 &= \mathbf{D}_1(\mathbf{I} + \mathbf{F}_1), & \mathbf{F}_2 &= \mathbf{I} - \mathbf{AD}_2 \\ &\vdots & &\vdots \\ \mathbf{D}_i &= \mathbf{D}_{i-1}(\mathbf{I} + \mathbf{F}_{i-1}), & \mathbf{F}_i &= \mathbf{I} - \mathbf{AD}_i. \end{aligned} \quad (4.33)$$

It may be noted that the matrix  $\mathbf{F}_i = \mathbf{I} - \mathbf{A}\mathbf{D}_i$  is equal to  $\mathbf{F}_0^{2^i}$ :

$$\begin{aligned}
 \mathbf{F}_i &= \mathbf{I} - \mathbf{A}\mathbf{D}_i \\
 &= \mathbf{I} - \mathbf{A}\mathbf{D}_{i-1}(\mathbf{I} + \mathbf{F}_{i-1}) \\
 &= \mathbf{I} - (\mathbf{I} - \mathbf{F}_{i-1})(\mathbf{I} + \mathbf{F}_{i-1}) \\
 &= \mathbf{I} - \mathbf{I} + \mathbf{F}_{i-1} - \mathbf{F}_{i-1} + \mathbf{F}_{i-1}^2 \\
 \therefore \mathbf{F}_i &= \mathbf{F}_{i-1}^2 = \mathbf{F}_{i-2}^4 = \dots = \mathbf{F}_0^{2^i}.
 \end{aligned} \tag{4.34}$$

Hence, it follows that

$$\mathbf{D}_i = \mathbf{A}^{-1}(\mathbf{I} - \mathbf{F}_0^{2^i}). \tag{4.35}$$

The above equation shows that  $\mathbf{D}_i$  approaches  $\mathbf{A}^{-1}$  with a rapid convergence. However, a sufficient condition for convergence to occur is that the norm of the error sequence be less than unity, i.e.  $\|\mathbf{F}_0\| = \|\mathbf{I} - \mathbf{A}\mathbf{D}_0\| < 1$ . This implies an adequate initial estimate of the inverse matrix.

The method of successive approximation can be computed by lifting the parentheses from (4.35), resulting in

$$\begin{aligned}
 \mathbf{D}_i &= \mathbf{D}_{i-1}(\mathbf{I} + \mathbf{F}_{i-1}) \\
 &= \mathbf{D}_{i-1} + \mathbf{D}_{i-1}(\mathbf{I} - \mathbf{A}\mathbf{D}_{i-1}),
 \end{aligned} \tag{4.36}$$

where the second summand performs a correction to the first.

It may be expedient to form the successive squaring of the matrix  $\mathbf{F}_0$ , such that the terms  $\mathbf{F}_1 = \mathbf{F}_0^2$ ,  $\mathbf{F}_2 = \mathbf{F}_1^2 = \mathbf{F}_0^4$ , ..., are easily utilized in (4.35). One can then easily set a termination criteria for the iterative process by setting  $\|\mathbf{F}_i\| < \varepsilon$ , where  $\varepsilon$  is the desired accuracy level.

It is generally well known that little can be done to avoid large computational errors for ill-conditioned systems. However, it is sometimes possible to reformulate the simultaneous equations such that the ill-conditioned properties are minimized. Since the upper bounds of the errors in the linear solution associated with  $\mathbf{Ax} = \mathbf{b}$  are typically proportional to the condition number  $\kappa(\mathbf{A})$ , then diagonal scaling is often used in an attempt to make  $\kappa(\mathbf{A})$  near unity for the scaled system, i.e.,

$$\mathbf{A} \leftrightarrow \tilde{\mathbf{A}} = \mathbf{DAE}, \quad (4.37)$$

where  $\mathbf{D}$  and  $\mathbf{E}$  are nonsingular diagonal matrices.

If one were to revise Turin's formulation by simply redefining a single variable, specifically the time component, then one may obtain the following. Let  $\tilde{u} = -cu$  be the substitution in (4.19), then one obtains:

$$h = (x - \hat{x}_0), k = (y - \hat{y}_0), \tilde{u} = c(\hat{\tau}_0 - \tau) \quad (4.38)$$

$$\begin{bmatrix} \sum \alpha_i^2 \Delta x_i^2 & \sum \alpha_i^2 \Delta x_i \Delta y_i & \sum \alpha_i^2 \Delta x_i \\ \sum \alpha_i^2 \Delta x_i \Delta y_i & \sum \alpha_i^2 \Delta y_i^2 & \sum \alpha_i^2 \Delta y_i \\ \sum \alpha_i^2 \Delta x_i & \sum \alpha_i^2 \Delta y_i & \sum \alpha_i^2 \end{bmatrix} \begin{bmatrix} h \\ k \\ \tilde{u} \end{bmatrix} = - \begin{bmatrix} \sum \alpha_i^2 \Delta x_i f_i(\hat{x}_0, \hat{y}_0, \hat{\tau}_0) \\ \sum \alpha_i^2 \Delta y_i f_i(\hat{x}_0, \hat{y}_0, \hat{\tau}_0) \\ \sum \alpha_i^2 f_i(\hat{x}_0, \hat{y}_0, \hat{\tau}_0) \end{bmatrix} \quad (4.39)$$

$$\text{i.e. } \tilde{\mathbf{A}} = \mathbf{DAE}, \quad (4.40)$$

where

$$\mathbf{D} = \mathbf{I}, \text{ and } \mathbf{E} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1/c \end{bmatrix}. \quad (4.41)$$

Thus, the iterative procedure outlined by Turin is now used with the exception that the solution set  $(h, k, \tilde{u})$  is substituted into the expression

$$|h| + |k| + |\tilde{u}| < \varepsilon \quad (4.42)$$

to evaluate the error constraint, and the parameter updates are subsequently obtained by using

$$\hat{x}'_0 = \hat{x}_0 + h, \hat{y}'_0 = \hat{y}_0 + k, \hat{\tau}'_0 = \hat{\tau}_0 - \frac{\tilde{u}}{c}. \quad (4.43)$$

To illustrate the conditioning of the design matrix, assume that three listening stations are distributed at the following universe transverse mercator (UTM) coordinates.

Table 4.1 LS UTM Coordinates

LS	Northing (m)	Easting (m)
1	710433.442397477	5660017.199292434
2	707957.554803613	5662795.039588497
3	710109.613877999	5663004.098975709

The coordinates correspond to the north-east quadrant of Calgary, Alberta. The MS is assumed to be at the mean center of the listening stations, i.e.,

$$(x, y) = (709500.203693030, 5661938.779285550) \text{ m.}$$

This results in a HDOP of 1.24, and the initial position estimate or starting point will have an offset from the true location by 100 m in both the East and North components. The condition numbers of the design matrices of (4.25) and (4.39) for the first iterate are then  $\kappa(\mathbf{A}) = 8.63 \times 10^8$  and  $\kappa(\tilde{\mathbf{A}}) = 2.98$ , respectively. Hence, it is preferable to use the revised design matrix.

#### 4.5 Direct TOA Substitution Using Circular Format

At roughly the same time that Turin's benchmark paper was published, there was a submission by Warren *et al.* [73] in which the narrowband trilateration process was examined for fleet management. The positional computation from three time interval measurements under ideal conditions (i.e. no measurement errors, especially multipath

effects) is shown below. Rather than performing the solution in an iterative least squares procedure, the equations were reformatted to work in a direct circular (i.e. TOA) format.

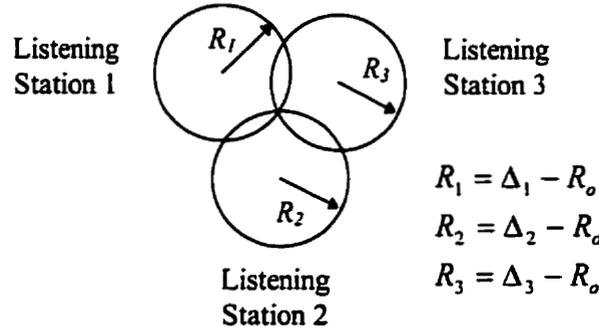


Figure 4.3. Illustration of circular format location algorithm.

These researchers had an additional time parameter (omitted below) in their equations that was dependent on the method of time synchronization among all the listening stations. It is assumed that a time of arrival measurement  $t_i$  is made at the  $i^{\text{th}}$  listening station and is then related to the actual baseline for the vehicle and the listening station by the relation

$$\frac{R_i}{c} = \partial t_i - t_o, \quad (4.44)$$

where  $R_i$  denotes the actual baseline,  $\partial t_i$  is the measured time of arrival,  $t_o$  is the unknown time of transmission (which is common to all listening stations), and  $c$  is the speed of light:

$$\Rightarrow R_i = \Delta_i - R_o \quad (4.45)$$

where  $\Delta_i = c\partial t_i$ , and  $R_o = ct_o$ ,

$$\begin{aligned} R_i &= \Delta_i - R_o \\ &= c\partial t_i - ct_o \\ &= c(\partial t_i - t_o) \end{aligned} \quad (4.46)$$

$$\Delta_i - R_o = \sqrt{(x - x_i)^2 + (y - y_i)^2}, \quad i = 1, 2, 3. \quad (4.47)$$

Expanding (4.47) one obtains

$$\Delta_i^2 - 2\Delta_i R_o + R_o^2 = x^2 - 2xx_i + x_i^2 + y^2 - 2yy_i + y_i^2, \quad i = 1, 2, 3. \quad (4.48)$$

Now if one were to choose a reference of the three listening stations in order to form differences, for example, the first station may be chosen as the reference so that when  $i = 1$  is subtracted from the other two possible equations above, one obtains:

$$\begin{aligned} \Delta_i^2 - \Delta_1^2 + 2R_o(\Delta_1 - \Delta_i) &= 2x(x_1 - x_i) + (x_i^2 - x_1^2) + 2y(y_1 - y_i) + (y_i^2 - y_1^2) \\ 2(x_1 - x_i)x + 2(y_1 - y_i)y &= 2(\Delta_1 - \Delta_i)R_o + C_i, \end{aligned} \quad (4.49)$$

where

$$C_i = \Delta_i^2 - \Delta_1^2 + x_1^2 - x_i^2 + y_1^2 - y_i^2 \quad \text{for } i = 2, 3. \quad (4.50)$$

Rewriting (4.49) as simultaneous equations for  $i = 2, 3$  one gets

$$\begin{bmatrix} 2(x_1 - x_2) & 2(y_1 - y_2) \\ 2(x_1 - x_3) & 2(y_1 - y_3) \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 2(\Delta_1 - \Delta_2)R_o + C_2 \\ 2(\Delta_1 - \Delta_3)R_o + C_3 \end{bmatrix}. \quad (4.51)$$

Now to determine  $(x, y)$ , let

$$\mathbf{A} = \begin{bmatrix} 2(x_1 - x_2) & 2(y_1 - y_2) \\ 2(x_1 - x_3) & 2(y_1 - y_3) \end{bmatrix}, \quad (4.52)$$

thus

$$\begin{bmatrix} x \\ y \end{bmatrix} = \frac{1}{|\mathbf{A}|} \begin{bmatrix} 2(y_1 - y_3) & 2(y_2 - y_1) \\ 2(x_3 - x_1) & 2(x_1 - x_2) \end{bmatrix} \begin{bmatrix} 2(\Delta_1 - \Delta_2)R_o + C_2 \\ 2(\Delta_1 - \Delta_3)R_o + C_3 \end{bmatrix}, \quad (4.53)$$

where the determinant  $D$  is given by

$$\begin{aligned} D = |\mathbf{A}| &= 2^2 [(x_1 - x_2)(y_1 - y_3) - (x_1 - x_3)(y_1 - y_2)] \\ &= 2^2 [y_1(x_3 - x_2) + y_2(x_1 - x_3) + y_3(x_2 - x_1)]. \end{aligned} \quad (4.54)$$

Then let

$$\begin{aligned} A_x &= 2[(y_1 - y_3)(\Delta_1 - \Delta_2) + (y_2 - y_1)(\Delta_1 - \Delta_3)] / D \\ &= 2[y_1(\Delta_3 - \Delta_2) + y_2(\Delta_1 - \Delta_3) + y_3(\Delta_2 - \Delta_1)] / D \end{aligned} \quad (4.55)$$

and similarly let

$$\begin{aligned} b_x &= [(y_1 - y_3)C_2 + (y_2 - y_1)C_3] / D \\ &= 2\{y_1(\Delta_2^2 - \Delta_3^2) + y_2(\Delta_3^2 - \Delta_1^2) + y_3(\Delta_1^2 - \Delta_2^2) + (x_1^2 + y_1^2)(y_2 - y_3) + \\ &\quad (x_2^2 + y_2^2)(y_3 - y_1) + (x_3^2 + y_3^2)(y_1 - y_2)\} / D. \end{aligned} \quad (4.56)$$

Using (4.55) and (4.56) to solve for  $x$  and  $y$  above, one obtains

$$x = 2A_x R_o + b_x \text{ and similarly } y = 2A_y R_o + b_y, \quad (4.57)$$

where

$$A_y = 2[x_1(\Delta_2 - \Delta_3) + x_2(\Delta_3 - \Delta_1) + x_3(\Delta_1 - \Delta_2)] / D \quad (4.58)$$

$$\begin{aligned} b_y &= 2\{x_1(\Delta_3^2 - \Delta_2^2) + x_2(\Delta_1^2 - \Delta_3^2) + x_3(\Delta_2^2 - \Delta_1^2) + \\ &\quad (x_1^2 + y_1^2)(x_3 - x_2) + (x_2^2 + y_2^2)(x_1 - x_3) + (x_3^2 + y_3^2)(x_2 - x_1)\} / D. \end{aligned} \quad (4.59)$$

Now by substituting (4.57) into (4.48) with the index  $i = 1$ , one gets

$$\begin{aligned} \Delta_1^2 - 2\Delta_1 R_o + R_o^2 &= (2A_x R_o + b_x)^2 - 2x_1(2A_x R_o + b_x) + x_1^2 + \\ &\quad (2A_y R_o + b_y)^2 - 2y_1(2A_y R_o + b_y) + y_1^2. \end{aligned} \quad (4.60)$$

It should be noted that (4.60) contains known quantities with the exception of  $R_o$ . Now by expanding (4.60) and collecting terms with respect to  $R_o$ , one may generate the result

$$\begin{aligned} \{ R_o^2 [1 - 4(A_x^2 + A_y^2)] + R_o [4A_x(x_1 - b_x) + 4A_y(y_1 - b_y) - 2\Delta_1] \\ - (b_x - x_1)^2 - (b_y - y_1)^2 + \Delta_1^2 \} = 0. \end{aligned} \quad (4.61)$$

Solving the quadratic expression above for  $R_o$ , one obtains the result

$$\begin{aligned}
 R_o = & \frac{2A_x(x_1 - b_x) + 2A_y(y_1 - b_y) - \Delta_1}{1 - 4(A_x^2 + A_y^2)} \\
 & \pm \left\{ (x_1 - b_x - 2\Delta_1 A_x)^2 + (y_1 - b_y - 2\Delta_1 A_y)^2 \right. \\
 & \left. - 4 \left[ A_x(b_y - y_1) - A_y(b_x - x_1) \right]^2 \right\}^{\frac{1}{2}} / \left\{ 1 - 4(A_x^2 + A_y^2) \right\}.
 \end{aligned} \tag{4.62}$$

Thus, once  $R_o$  is obtained, then  $(x, y)$  can be determined from (4.57). The  $\pm$  sign ambiguity represents the same ambiguity as two intersecting hyperbola which produce two possible solutions. Warren suggests that a fourth listening station will resolve this ambiguity, yet there is an intuitive solution to resolving this problem that one may employ. Recall that the formulation is based on solving the radial baseline  $R_o$  which is essentially the time difference of the signal transmission and reception. Now typically the signal reception time has external and internal measurement errors, in which multipath effects tend to increase the effective reception time and hence propagation time. Thus, the intuitive selection of the two possible sets may be made by minimizing the radial baseline or propagation time, so the  $\pm$  sign is determined by  $\min \{|R_o|\}$ . Due to the external and internal measurement errors, three potential solutions exist from the three listening stations, each with two possible candidates. Thus, an individual solution may be utilized for the MS position estimate or a weighted combination of the three solutions can be used.

#### 4.6 Simulation of Two-Dimensional IS-54-B Positioning

The TOA estimation process consisted of simulating the baseband transmission of both normal traffic bursts and shortened bursts, where an average TOA estimate of the shortened burst is used. Since the mSCID process obtained better ranging performance with the MLSR sequences in Chapter Two, the TOA information was estimated solely by

the mSCID method. A three-ray channel model with complex additive white Gaussian noise was assumed for each transmission path, where the discrete arrivals are characterized as

$$h(t) = \sum_{i=1}^3 \alpha_i \delta(t - \tau_i).$$

The discrete arrival times per transmission path are held constant at  $\tau_1 = \tau_{\text{LOS}}$ ,  $\tau_2 = \tau_1 + 1.5 \mu\text{s}$ , and  $\tau_3 = \tau_1 + 3 \mu\text{s}$ , where  $\tau_{\text{LOS}}$  is determined from the associated baseline. The arrival amplitudes,  $20 \log_{10} \alpha_i$ , are normal with mean  $\mu_i$  and variance  $\sigma_i^2$ , where  $\mu_1 = 0 \text{ dB}$ ,  $\mu_2 = -3 \text{ dB}$ ,  $\mu_3 = -10 \text{ dB}$ , and  $\sigma_1^2 = 2 \text{ dB}$ ,  $\sigma_2^2 = \sigma_3^2 = 6 \text{ dB}$ . The phase of the multipath components is uniformly distributed between 0 and  $2\pi$ . The MS is then randomly placed in the designated coverage area of the serving base station, shown as cell A in Fig. 4.4. A one second interval (i.e. 25 RDTC frames at full rate assignment) was assumed at each location for the normal traffic bursts, where 250 locations were generated resulting in 12,500 observations. Similarly, 250 MS locations were generated for the shortened burst transmissions, with 12,500 observations in total. The listening stations are co-located with the base stations, which are assumed to have omni-directional antennas. The cell radius,  $R$ , correspond to a -95 dBm downlink received signal strength contour for a 30 W ERP, a path loss exponent of 4, and a channel assignment of 367 (i.e. IS-54-B channel simulator). Hence, the cell radius is approximately 16.2 km.

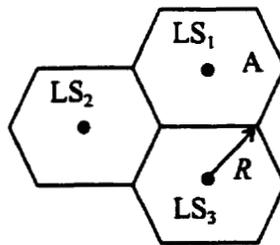


Figure 4.4. Listening Station distribution for position estimation.

A class 3 mobile phone is assumed, which has a 28 dBm maximum ERP. The LS receiver noise floor is set to -116 dBm, and all transmissions occur on channel 367 (i.e. an uplink frequency of 836.010 MHz). The MS transmission level is adjusted for an approximate received power level of -73 dBm at the serving base station, according to the transmission levels outlined in Table 3.3. If the required power level exceeds the allowed limits then the transmission level is set to the appropriate bound (i.e. level 0 or 10). Other parameter assignments in the simulation are time slot 3, CDVCC 1,  $f_s = 16 \times 24.3$  kHz,  $N_{FFT} = 256$ ,  $N = 17$ , and  $M = 12$ . One may note that using (2.40)

indicates that the observations will be strongly coherent, since  $\frac{17}{(12-1)16} T_{symbol} > 1.5 \mu s$ .

Transmissions from an indoor environment were not considered since the additional loss would limit the effective reception area for positioning purposes, without additional gain being required at the listening stations. Estimates were generated from both the conditioned version of Turin's multilateration algorithm and that of [73]. The mobile's estimated location was then compared to its true location, and the radial error computed. The cumulative distribution of the radial error of the estimated locations is then plotted.

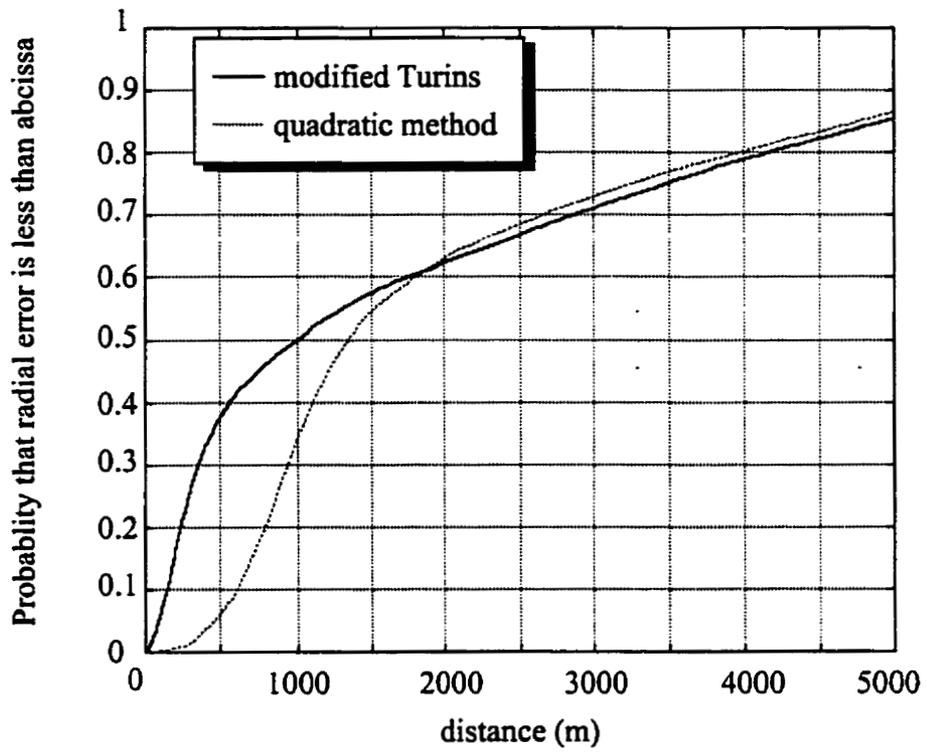


Figure 4.5. Position error distribution for normal RDTTC bursts.

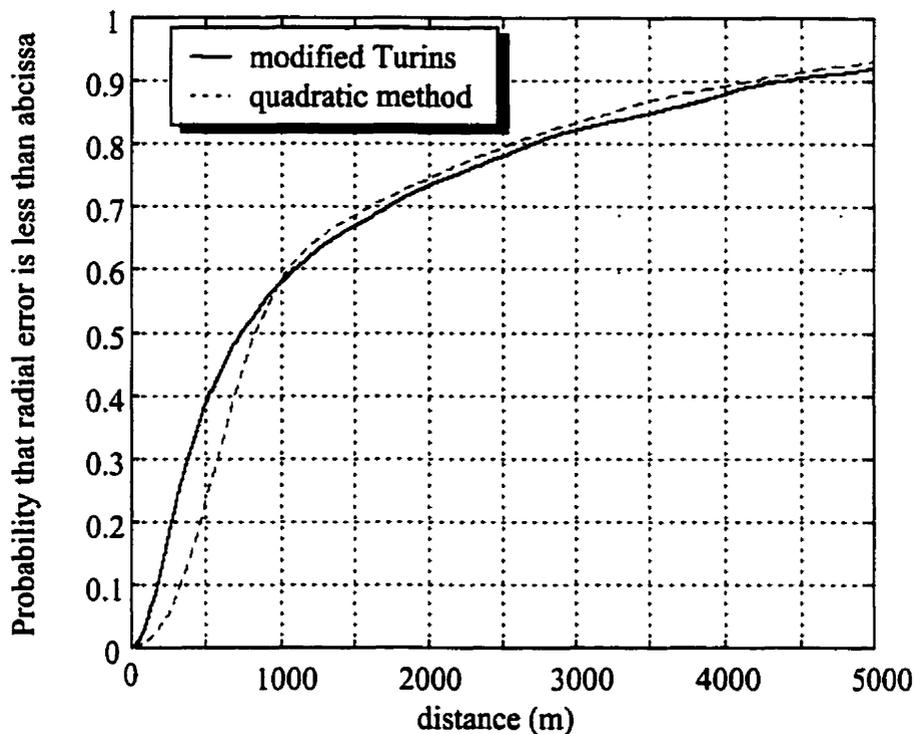


Figure 4.6. Position error distribution for shortened bursts.

The large radial errors occur from the poor TOA estimates in low SNR conditions, which is further compounded by poor geometry. Recall that the HDOP is the ratio of the *RMS* position error to the *RMS* ranging error, and the HDOP typically varied from 1 to 30. Although increasing the sensitivity of the listening stations; and/or the MS's transmit power, will reduce TOA errors of some path estimates, other estimates will still suffer poor resolution due to the large baselines. If one examines the radial error under better geometrical conditions, where the cumulative error distribution is reevaluated for observations with an  $\text{HDOP} \leq 3$ , we obtain the results illustrated in Fig. 4.7 and Fig. 4.8.

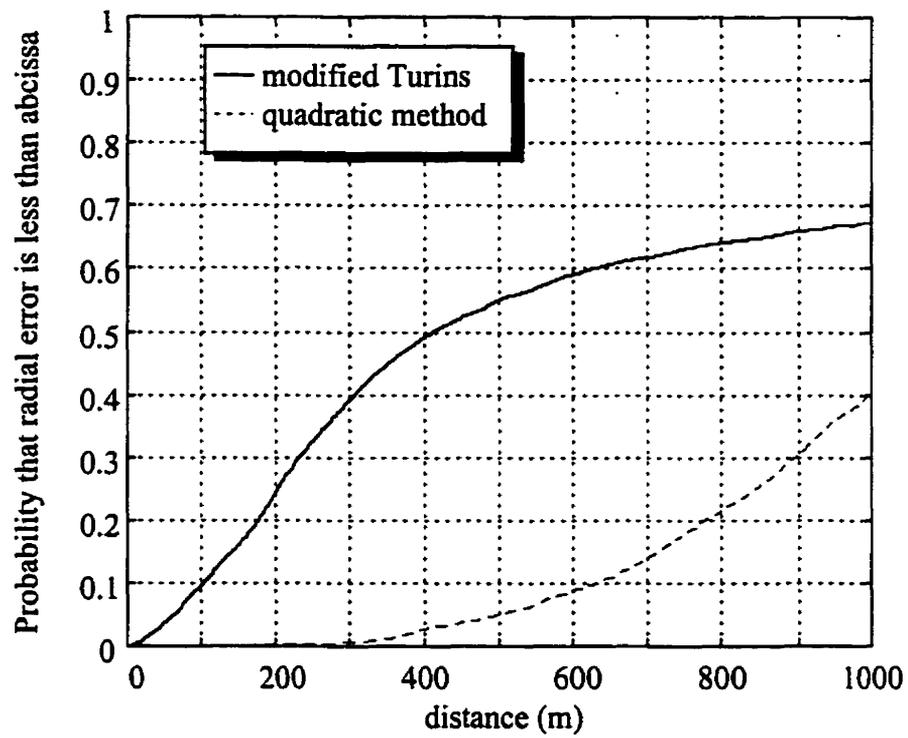


Figure 4.7. Constrained ( $\text{HDOP} \leq 3$ ) position error distribution for normal RDTC bursts.

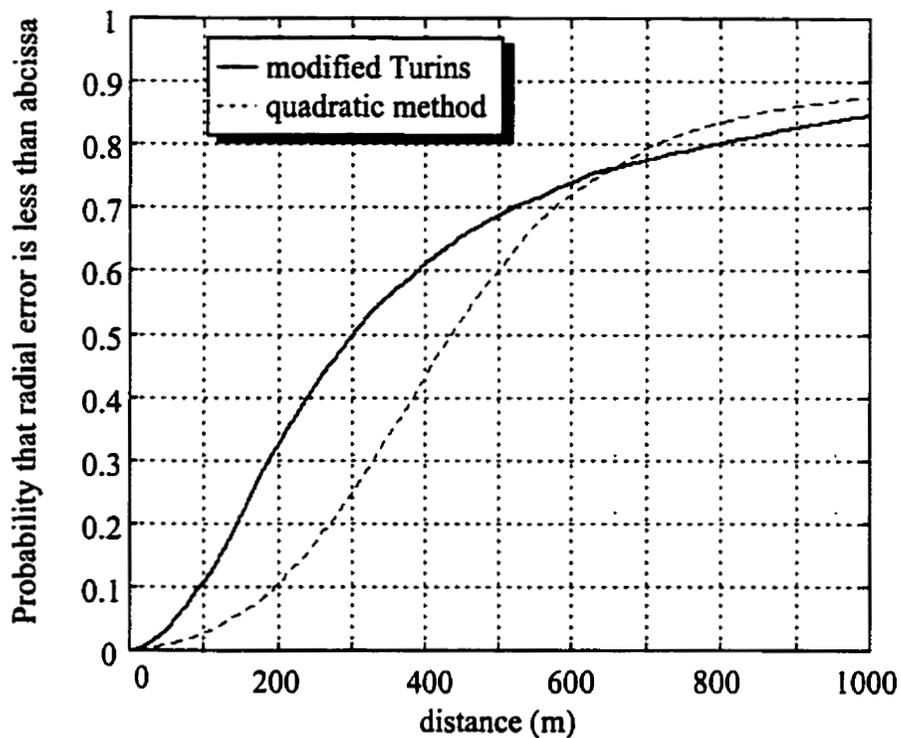


Figure 4.8. Constrained ( $\text{HDOP} \leq 3$ ) position error distribution for shortened bursts.

Using the shortened burst has the advantage of utilizing more information from the training sequence, however, the disadvantage is that under normal network operations it is transmitted relatively infrequently, unless BS operations are modified for a "locate" mode. Since an ensemble average is performed on the shortened burst to obtain a TOA estimate, one may perform a similar average of several burst periods on a normal RDTC. Fig. 4.9 illustrates the obtained mean radial error over a one second interval, i.e. 25 frames with two burst periods per frame (i.e. full rate assignment).

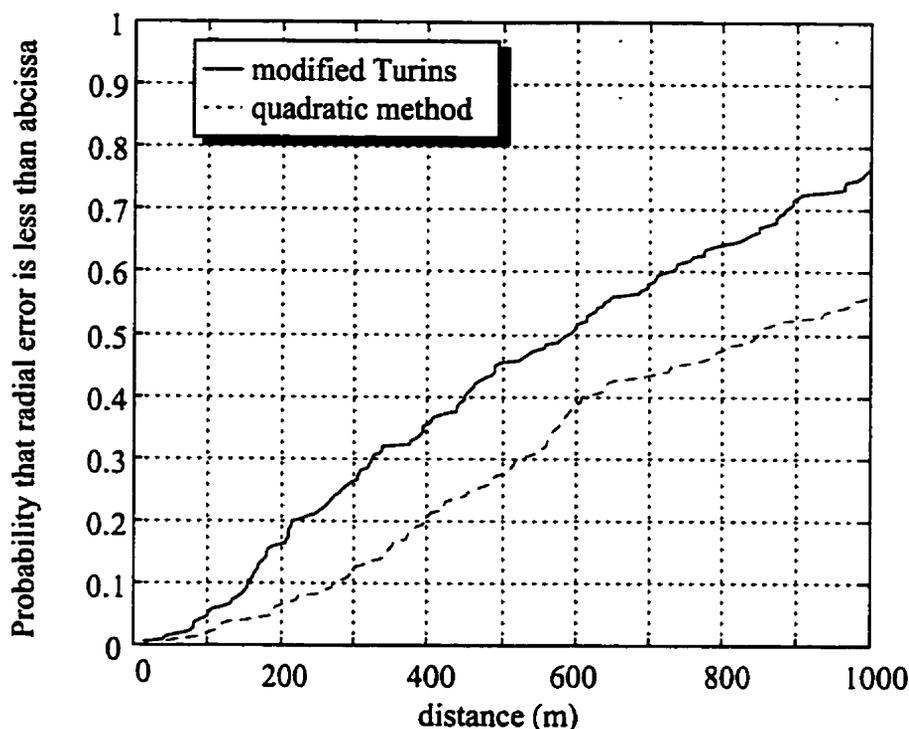


Figure 4.9. Constrained ( $\text{HDOP} \leq 3$ ) position error distribution for averaged normal RDTTC bursts.

It was assumed that averaging location estimates over several frames would produce a lower radial error, however, blunders can unduly skew the obtained location. Hence, one must apply an appropriate blunder detection scheme prior to performing a weighted average. Also, the number of averaged sequences used to either obtain an averaged TOA estimate or an averaged location estimate will be a function of the MS's estimated speed.

#### 4.7 Master Time Reference Errors

The previous simulation assumed perfect time synchronization among the listening stations, however, this is not achievable in the real world. High-end GPS receivers can obtain software corrected relative time resolutions of 50 ns for standard positioning service (SPS), but one cannot ensure that all receivers have a common view

of the same GPS satellites. A random timing error is now introduced at each LS, which has a zero mean and standard deviation  $\sigma_\tau = 100$  ns.

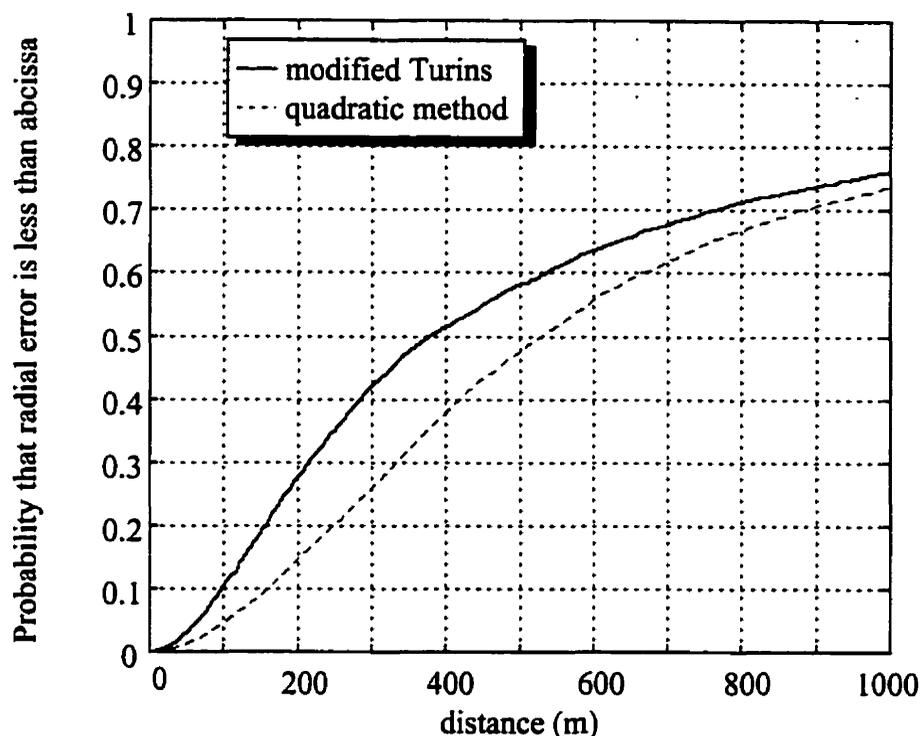


Figure 4.10. Constrained ( $\text{HDOP} \leq 3$ ) position error distribution for shortened bursts and  $\sigma_\tau = 100$  ns.

As expected, the above figure clearly illustrates that the radial error budget is proportional to the synchronization error of the common LS timing source. Hence, the system clocks must be disciplined to a stable and accurate reference such that the error budget is dominated by the multipath effects. This timing constraint will also affect handset-based geolocation systems.

## **Chapter 5: Conclusions**

### **5.1 Summary of the Thesis**

A viable cellular location method has been presented that supports existing digital cellular mobile stations and networks. The multipath rejection algorithm utilizing super-resolution processing can obtain the required accuracy mandated by the FCC under geometric constraints and increased SNR, either by increasing the handset's transmission level and/or increasing the receiver sensitivity of the listening stations. The modified SCID method has the benefits of:

- i) processing uplink signaling for TOA measurements with unknown transmission times;
- ii) reduced SNR sensitivity due to known burst periods for TDMA systems, allowing a larger set of listening stations to participate in the measurement process;
- iii) improved indoor performance due to reduced SNR sensitivity;
- iv) flexibility of selecting measurement subsets to improve the solution HDOP due to the increased observables.

In Chapter 2, an overview of super-resolution processing; both bearing and time estimation, by past researchers from the University of Calgary was presented. The foundation of the TOA estimation process was outlined, and subsequently refined. The modified SCID process allowed improvements in the relative TOA adjustments by restricting the candidate root set to a phase corridor on the complex plane. A bias estimation process was developed to reduce the effects of forward-backward smoothing on the root-MUSIC algorithm. The original and modified versions of the SCID process were then compared on computer generated wideband data sets for multipath reception, and on indoor measurements.

In Chapter 3, an overview of the AMPS and IS-54-B CMRS was presented. Potential deterministic code sequences were outlined for TOA estimation, along with potential issues for the location process.

In Chapter 4, the results of Chapter 2 were exploited and applied to the NADC air-interface signaling, allowing two-dimensional positioning of unmodified handsets. The shortened burst and normal traffic bursts were examined for TOA estimation, and position determination using both a direct circular format algorithm and a linearized least squares algorithm. Time synchronization errors among the listening stations was also investigated, where the radial error budget becomes proportional to the synchronization error of the utilized common clocks. The obtained cumulative error distribution does not provide sufficient statistics for the 250 randomly generated MS locations since the HDOP was significantly high. This may be remedied by including more observations (i.e. listening stations) in the position determination.

## **5.2 Proposed Topics of Further Research and Other Thoughts**

It should be noted that the effects of cochannel and adjacent channel interference have not been addressed in this thesis. Only a single MS with no interferers was considered, thus, the proposed method or any other network-centric method, remains sensitive to cochannel interference. The modeling of multiuser interference is not a trivial issue since it is dependent on network parameters and terrain, yet should be investigated to reevaluate expected performance. Analysis of successively more complicated data sequences would be required to provide a better understanding of algorithm behavior, which will lead to further refinements. Furthermore, since wireless service providers continually tune their networks to obtain a desired self interference performance, the process/system will have to be tailored to each individual cellular network it is deployed in. Hence, in depth knowledge of the overall location process is required for the real world.

Clearly, the two dominant factors that affect the net performance of this cellular location method are the determined time lobe used in the process, and the mode estimate used in the root-MUSIC algorithm. Many post-processing methods exist for low SNR signal interception, however, the method must be implemented near real-time due to inter-network latency issues for the end application. Catastrophic degradation in performance occurs when the number of sources is overestimated, and one cannot rely on the CIR delay profile to be narrow for the case when the sources are underestimated. One can perform an ad hoc adjustment to the mode estimates in an attempt to reduce the error variance and bias in the resultant TOA estimates, however, additional methods should be investigated that provide more accurate mode estimates. These methods should also be computationally efficient, similar to those approaches that exploit the obtained singular value distribution.

### **5.2.1 Reliability**

Although the FCC wishes location technologies to provide a positional accuracy of 125 m *DRMS* for all possible scenarios, this is not a realistically achievable goal. Even proven technologies such as GPS, which have the capability of providing the required resolution cannot provide the necessary positional updates for all cases, whether in rural or urban environments. There even exists in the literature misconceptions about the sub-meter accuracy achievable with differential GPS. This mode of operation helps mitigate atmospheric propagation effects and the intentional degradation of the empheris data and satellite clock phase, but does not improve TOA values in a multipath environment or increase the number of observables when signal masking occurs. Thus, passive location technologies based on inherent CMRS signaling will provide the highest probability of interception despite their inherent resolution limitations. The issue then becomes one in which a plausible location is provided with a potentially higher horizontal error or no location is provided at all. Since the primary focus of many

regulatory agencies is on wireless E911 capability, then obviously it would be better to provide a plausible location as emergency response teams would still be able to locate the wireless caller rather than not at all. In fact, most emergency services are only concerned with response times, i.e. the time required for vehicle dispatch and route guidance [74]. Once the emergency vehicles are in the vicinity then the response team can quickly find the caller as they have had prior training and experience in locating wireline 911 callers.

Presently, location technologies prefer using least squares in the positioning algorithm because statistics may be readily obtained from the covariance matrix. There are numerous other positioning algorithms, both iterative and closed-form, that provide similar results but nearly all assume that the measurement errors, either internal or external, are independent identically distributed (*iid*) with zero mean. However in all location technologies, biases occur from discrete component drifts and aging even though the location technology may be co-located with the cellular base station in a temperature regulated environment. It should also be noted that drift errors will not track per listening station so applying differencing techniques in the position algorithm will not always reduce measurement errors. Although these biases may exhibit Gaussian properties over longer time intervals, the short bursty nature of CMRS will exhibit non-zero means, which in turn will affect the position solution. These biases then become more critical due to the time-bandwidth limitation of CMRS. This is the reason that most location technologies must perform calibration every few minutes. If the positioning algorithm is based on differencing techniques, the calibration process can become quite complex as error adjustments will have to be distributed among all listening stations used in the measurement process. In addition, this calibration can either be achieved individually in an internal/onboard process or in an external/localized process. If onboard calibration is conducted, then a swept reference source will periodically have to be injected into the receiver and the output characteristics stored in non-volatile memory which can be later retrieved in the processing steps for the received observable. In an external calibration process, the system would require a stationary RF emitter or beacon

at known coordinates that would periodically broadcast pseudo-messages (similar to the CRMS being monitored) for the localized listening stations. The measurement errors thus obtained would then be subsequently distributed among the listening stations according to some stochastic process. This approach assumes that the pseudo-messages are sent on the allocated frequencies of the Mobile Transmit band. However, if this calibration process is overly long, network degradation will occur as the pseudo-messaging will occupy traffic or control channels and deny access to paying subscribers. The alternative is for wireless carriers to dedicate a single channel for the calibration process. Typically, wireless carriers do not utilize the boundary control channels that separate the A and B bands in the AMPS or NADC systems (i.e. channels 333 and 334), therefore the calibration process can be conducted without any mutual interference.

Some researchers feel that calibration can be readily achieved by utilizing the forward signaling channels of base stations since FOCC system overhead messages are sent approximately every 0.8 seconds [75]. However, this method of calibration is not entirely accurate as the Mobile Transmit and Mobile Receive bands are separated by a 45 MHz guard band to minimize intermodulation products, image components, and amplifier/mixer saturation. Therefore, the frequency characteristics obtained from the FOCC would have to be translated to give an estimate of the lower frequency band characteristics. However, the discrete and active components of the listening station are frequency dependent and will drift at different rates. Furthermore, an RF isolation design problem exists since the calibration unit is in close proximity to a high-powered emitter.

To avoid frequent calibration, research should be conducted into developing positioning algorithms that account for non-zero mean (e.g. ellipticity) measurements in the TDOA, TOA, or AOA observables. This may translate into forcing the MS to provide a larger data ensemble through frequent non-autonomous registrations (whether on RECC or DCCH channels) or by using several positioning algorithms and correlating their solutions to adjust for measurement biases. Select positioning algorithms may then

be used such that they complement each other in their respective regions where their individual solutions are very sensitive to initial conditions, biases, and measurement errors. The joint estimator accuracies may also be used to improve the confidence region when correlated to each other.

Other alternatives exist for a globally optimal location solution, and should be investigated due to the fact that most positioning algorithms are iterative, i.e. the methods typically apply constrained gradient searches or “hill-climbing” algorithms. Hill-climbing algorithms use the iterative improvement technique, which is applied to a single point in the search space (i.e. the current point). A new point is then selected in the neighborhood of the current point based on a given objective or merit function and then becomes the current point in the next iterate. These methods will then terminate if no further improvement is achievable (i.e. it has reached a local or global minimum/maximum), although the success or failure of the process is dependent on the starting point. In addition, there is no information regarding the relative error (with respect to the global optimization) of the converged solution. This becomes quite significant in the positioning of handsets because multiple local optima (i.e. location images) exist in close proximity to the true location and can easily pull the search point away from the true position in a single iteration [76]. Therefore, it may be desirable to utilize evolutionary programs such as Genetic Algorithms (GA) to overcome the limitations of present iterative techniques, especially since they contain a population of potential solutions for each iterate rather than a single point of the search space. Thus, at each iterative step the “good” solutions are allowed to continue while the “bad” solutions are removed based on a merit function. Other aspects of GA such as crossover and mutation between some of the potential solutions may be allowed or inhibited, depending on the required objectives. In essence, evolutionary programs have an advantage over simple iterative techniques in that the solution need no longer be dependent on the starting point, however, the computational requirements increase dramatically.

### **5.2.2 Signal Interception**

There are numerous location technologies targeting the CMRS market as outlined in the Driscoll survey [7], yet very few of these technologies have provided the necessary accuracy that the FCC is demanding. Of these few technologies with the potential resolution, the consensus of the CTIA and the FCC has been that the viable location technology will be a system that utilizes TDOA positioning techniques due to achievable accuracy and deployment costs, of these techniques.

However, a fundamental drawback of all network-centric based solutions is that the equipment is expected to be co-located with the cellular base station equipment and utilize the RF front-end equipment in order to reduce deployment costs. This type of network overlay architecture will run into signal interception problems due to present RF coverage design methodologies. The underlying principle of the cellular architecture is the frequency reuse capability through antenna beamforming and transmit power regulation. In essence, the network has been optimized to provide a specified grade of service for subscribers and is not adequate for RF emitter positioning because signal reception is now required at multiple sites rather than the minimal number required for seamless service for the subscriber. Hence, modifications will have to be conducted on the wireless networks to provide the capability of multiple signal reception by either modifying existing antenna coverage or adding separate antennas for the location technology. In addition, modifications to the air-interface may be required to allow cellular base stations to increase the handset's allowable transmit power level (e.g. the proposed Power-Up Function for IS-95-B [77]) even though network degradation would occur due to cochannel and adjacent channel interference.

### **5.2.3 Network Integration**

Presently wireless location technologies can either be network-centric or handset-based (pseudo-standalone), and although recent proposed location technologies prefer the

standalone solution due to its ease of implementation, there are significant disadvantages. The largest disadvantage of MS-based solutions is that there are over 50 million legacy handsets in North America that cannot be integrated into this type of solution, and subscribers would be reluctant to purchase new handsets just to obtain the location capability. If this type of solution is forced onto subscribers then the MS costs would have to be subsidized. The additional issue then arises of whom would subsidize the phasing out of the old handsets. Should wireless carriers, OEM vendors, or government agencies cover these net costs? Or will these costs be broken down based on wireless subscriber base, wireless and wireline subscriber base, PSAP jurisdictional coverage, etc.? MS-based solutions that incorporate GPS systems will have a large amount of outage in urban environments [78-80], making it impractical for E911 applications. There are numerous other disadvantages that MS-based systems will suffer including increased weight and size, and reduced battery life, but one significant problem occurs if the location of the MS is required without the user's knowledge.

Network-centric or MS-based solutions that utilize the ISM band, not to confused with PCS technology, are cost prohibitive due to establishing a network for RF coverage and backhauling the information to a central processing site or host. An additional problem occurs if the ISM-based system is not standardized, where such systems can interfere with each other as transmit power levels are no longer kept at Part-90 levels [81].

An issue that has not been addressed regarding wireless location systems, whether handset or network based, is network management and data routing requirements. An overlay network will be required for OA&M in North America as most OEM vendors do not follow a standardization for intersystem interfacing. Thus, the system must handle large traffic loads as it will be required to transport all TOA observables (or UTM coordinates if the position determination is performed at the handset) to the central processing site for subscriber association and appropriate data handling. This constitutes

a large traffic load even though the TOA observables (or geographical coordinates) may be compressed to small data lengths. Thus, the network architecture will have to be scaleable to accommodate present and future traffic loads. Furthermore, depending on the service provided, e.g. E911, fault tolerance may be critical in the architecture design to provide the degree of reliability expected of wireline/wireless carriers and government agencies.

It should be noted that network loading will also occur in the CMRS network besides the location technology network. Increased traffic will occur on transport facilities linking the BS, MSC, HLR, and VLR due to frequent registrations, shortened bursts, etc. Therefore a maximum number of location updates per unit time should not be exceeded. This is difficult as the subscriber base increases every year, and as navigation services become more commonplace in industry. This problem may be alleviated if the CMRS standard committees adopt location service signaling to reduce unnecessary intra-network data exchanges.

Once a viable location technology is incorporated into the wireless service providers' features, whether handset or network based, there will remain the issue of information transfer to the designated PSAP for the application of wireless E911. There are three immediate points that must be addressed in regards to this information transfer which are:

- i) availability, timing and accuracy of the information provided;
- ii) data traffic management, i.e. synchronizing the calls and the corresponding location information for PSAP operator availability;
- iii) tracking of the calls through handoffs between base station sectors, cell sites, mobile switches, networks and CMRS air interfaces (e.g. dual mode/band systems such as AMPS, IS-54/IS-136, IS-95, etc.).

### **5.3 Positioning of Personal Communication Systems**

It is expected that many countries will follow suit with the FCC's ruling for wireless carriers to provide enhanced 911 services for their subscribers, but it appears that many are waiting to see how well an adopted location technology performs in a commercial network. This is similar to previous industry decisions in North America regarding conversion from analog cellular technology to digital technology. For example, many wireless carriers waited until a particular vendor technology was deployed by a competitor before deciding which technology should be adopted in their own networks. However, the industry leaders in CMRS location technology in North America will have extensive knowledge and experience in implementing their technology; from their successes and failures, allowing them to readily adapt to other CMRS standards.

## References

- [1] *To Ensure Compatibility with Enhanced 911 Emergency Calling Systems*. FCC Notice of Proposed Rulemaking. CC Docket No. 94-102, October 1994.
- [2] *Commission Seeks Additional Comments in Wireless Enhanced 911 Rulemaking Proceeding Regarding "Consensus Agreement" Between Wireless Industry Representatives and Public Safety Groups*. CC Docket No. 94-102, 61 FR 6963, February 1996.
- [3] *Revision of the Commission's Rules To Ensure Compatibility with Enhanced 911 Emergency Calling Systems*. Report and Order and Further Notice of Proposed Rulemaking. CC Docket No. 96-264, June 1996.
- [4] *Revision of the Commission's Rules To Ensure Compatibility with Enhanced 911 Emergency Calling Systems*. Report and Order and Further Notice of Proposed Rulemaking. CC Docket No. 97-402, December 1997.
- [5] *The Cellular Telecommunications Industry Association's Wireless 911 Statistics*, on the web page of CTIA, [www.wow-com.com](http://www.wow-com.com).
- [6] *Revision of Part 22 of the Commission's Rule Governing The Public Mobile Services*. CC Dockets 92-115, 94-357, January 1995.
- [7] *Survey Of Location Technologies To Support Mobile 9-1-1 (Edition 1.0)*, C.J. Driscoll & Associates. July 1994.
- [8] *CTIA E911 Workshop on Location Technology*, Washington DC. January 1997.
- [9] L.L. Hagerman, *Effects of Multipath on Coherent and Noncoherent PRN Ranging Receiver*, Aerospace Report No. TOR-0073(3020-03)-3, May 1973.
- [10] A. Polydoros, C.L. Weber, *Analysis and Optimization of Correlative Code-Tracking Loops in Spread-Spectrum Systems*, IEEE Transactions on Communications, Vol. 33, No. 1, pages 30-43, January 1985.
- [11] A.J. Dierendonck, P. Fenton, T. Ford, *Theory and Performance of Narrow Correlator Spacing in a GPS Receiver*, Navigation: Journal of the Institute of Navigation, Vol. 39, No. 3, pages 265-283, Fall 1992.

- [12] B. Peterson, R.J. Hartnett, R. Fiedler, A. Nebrich, *Frequency Domain Techniques for Fast GPS Acquisition and Interference Detection/Rejection*, Navigation: Journal of the Institute of Navigation, Vol. 43, No. 3, pages 237-255, Fall 1996.
- [13] *EIA/TIA Interim Standard Cellular System Dual-Mode Mobile Station - Base Station Compatibility Standard*. IS-54-B, April 1992.
- [14] A.M. Bruckstein, T. Shan, T. Kailath, *The Resolution of Overlapping Echoes*, The IEEE Transactions on Acoustics, Speech, and Signal Processing, Vol. 33, No. 6, pages 1357-1367, December 1985.
- [15] H. Yamada, M. Ohmiya, Y. Ogawa, *Superresolution Technique for Time Domain Measurements with a Network Analyzer*, IEEE Transactions on Antennas and Propagation, Vol. 39, No. 2, pages 177-183, February 1991.
- [16] T. Manabe, H. Takai, *Superresolution of Multipath Delay Profiles Measured by PN Correlation Method*, IEEE Transactions on Antennas and Propagation, Vol. 40, No. 5, pages 500-509, May 1992.
- [17] L. Dumont, *Super-Resolution of Discrete Arrivals in a Spread Spectrum System*, M.Sc. Thesis, Dept. Of Electrical and Computer Engineering, The University of Calgary, Canada, July 1994.
- [18] L. Dumont, M. Fattouche, G. Morrison, *Super-resolution of multipath channels in a spread spectrum location system*, IEE Electronics Letters, Vol. 30, No. 19, pages 1583-1584, September 1994.
- [19] R. Klukas, *Angle Of Arrival Estimation In The Outdoor Radio Environment*, M.Sc. Thesis, Dept. Of Electrical and Computer Engineering, The University of Calgary, Canada, April 1993.
- [20] R. Klukas, M. Fattouche, *Line-of-Sight Angle of Arrival Estimation in the Outdoor Multipath Environment*, IEEE Transactions on Vehicular Technology, Vol. 47, No. 1, pages 342-351, February 1998.
- [21] D. Tholl, *Characterization Of The UHF Indoor Radio Propagation Channel*, M.Sc. Thesis, Dept. Of Electrical and Computer Engineering, The University of Calgary, Canada, September 1995.

- [22] J. Capon, *High-Resolution Frequency-Wavenumber Spectrum Analysis*, IEEE Proceedings, Vol. 57, No. 8, pages 1408-1418, August 1969.
- [23] S.Y. Kung, K.S. Arun, D.V. Bhaskar Rao, *State-space and singular-value decomposition-based approximation methods for the harmonic retrieval problem*, Journal of the Optical Society of America, Vol. 73, No. 12, pages 1799-1811, December 1983.
- [24] R. Kumaresan, D.W. Tufts, *Estimating the angles of arrival of multiple plane waves*, IEEE Transactions on Aerospace Electronic Systems, Vol. 19, No. 1, pages 134-139, January 1983.
- [25] A. Paulraj, R. Roy, T. Kailath, *Estimation of Signal Parameters via Rotational Invariance Techniques - ESPRIT*, XIX Allisomar Conference on Circuits and Systems, pages 83-89, November 1985.
- [26] R.O. Schmidt, *Multiple Emitter Location and Signal Parameter Estimation*, IEEE Transactions of Antennas and Propagation, Vol. 34, No. 3, pages 276-280, March 1986.
- [27] A.J. Barabell, *Improving the Resolution Performance of Eigenstructure-Based Direction -Finding Algorithms*, IEEE International Conference on Acoustics, Speech, and Signal Processing, pages 336-339, April 1983.
- [28] W.A. Gardner, *Simplification of MUSIC and ESPRIT by Exploitation of Cyclostationarity*, Proceedings of the IEEE, Vol. 76, No. 7, pages 845-847, July 1988.
- [29] J.T. Karhunen, J. Joutsensalo, *Sinusoidal Frequency Estimation by Signal Subspace Approximation*, IEEE Transactions on Signal Processing, Vol. 40, No. 12, pages 2961-2972, December 1992.
- [30] R. Kumaresan, D.W. Tufts, *Estimation of Frequencies of Multiple Sinusoids: Making Linear Prediction Perform Like Maximum Likelihood*, Proceedings of the IEEE, Vol. 79, No. 9, pages 975-989, September 1982.

- [31] R.O. Schmidt, R.E. Franks, *Multiple Source DF Signal Processing: An Experimental System*, IEEE Transactions on Antennas and Propagation, Vol. 34, No. 3, pages 281-290, March 1986.
- [32] S.K. Oh, C.K. Un, *Improved MUSIC algorithm for high-resolution array processing*, Electronic Letters, Vol. 25, No. 22, pages 1523-1525, October 1989.
- [33] C.S. Lee, M.H. Er, *Simple and Fast Method for Direction-Finding of Multiple Wideband Sources*, IEE Electronic Letters, Vol. 25, No. 22, pages 1522-1523, October 1989.
- [34] S.V. Pillai, B.H. Kwon, *Forward/Backward Spatial Smoothing Techniques for Coherent Signal Identification*, IEEE Transactions on Acoustics, Speech, and Signal Processing, Vol. 37, No. 1, pages 8-15, January 1989.
- [35] D.S. Hill, *Multiple signal DF using superresolution: a practical assessment*, Electronics & Communication Engineering Journal, pages 221-232, December 1990.
- [36] D. Kundu, *Modified MUSIC algorithm for estimating DOA of signals*, Signal Processing, Vol. 48, No. 1, pages 85-90, January 1996.
- [37] A. Delis, G. Papadopoubs, *Enhanced Forward/Backward spatial filtering method for DOA estimation of narrowband coherent signals*, IEE Proceedings of Radar, Sonar, Navigation, Vol. 143, No. 1, pages 10-16, February 1996.
- [38] J.E. Evans, J.R. Johnson, D.F. Sun, *High resolution angular spectrum estimation techniques for terrain scattering analysis and angle of arrival estimation*, Proceedings 1<sup>st</sup> IEEE Acoustics, Speech, and Signal Processing Workshop on Spectral Estimation, pages 134-139, 1981.
- [39] R. Kumaresan, *On the Zeros of the Linear Prediction-Error Filter for Deterministic Signals*, IEEE Transactions on Acoustics, Speech, and Signal Processing, Vol. 31, No. 1, pages 217-220, February 1983.
- [40] E.M. Dowling, D.A. Linebarger, R.D. DeGroat, H.Guan, *On the Elimination of Extraneous Roots*, IEEE Proceedings of ASILOMAR-29, pages 631-635, October 1996.

- [41] S. Haykin, *Adaptive Filter Theory (2<sup>nd</sup> Edition)*, Prentice-Hall, 1991.
- [42] T.J. Ulrych, R.W. Clayton, *Time series modeling and maximum entropy*, Phys. Earth Planet. Interiors, Vol. 12, pages 188-200, August 1976.
- [43] H. Akaike, *A New Look at the Statistical Model Identification*, IEEE Transactions on Automatic Control, Vol. 19, No. 6, pages 716-723, December 1974.
- [44] M. Wax, T. Kailath, *Detection of Signals by Information Theoretic Criteria*, IEEE Transactions on Acoustics, Speech, and Signal Processing, Vol. 33, No. 2, pages 387-392, April 1985.
- [45] M. Wax, I. Ziskind, *Detection of the Number of Coherent Signals by the MDL Principle*, IEEE Transactions on Acoustics, Speech, and Signal Processing, Vol. 37, No. 8, pages 1190-1196, August 1989.
- [46] B. Friedlander, *The root-MUSIC algorithm for direction finding with interpolating arrays*, Signal Processing, Vol. 30, No. 1, pages 15-29, January 1993.
- [47] K.M. Pasala, E.M. Friel, *Mutual Coupling Effects and their Reduction in Wideband Direction of Arrival Estimation*, IEEE transactions on Aerospace and Electronic Systems, Vol. 30, No. 4, pages 1116-1122, October 1994.
- [48] M. Fattouche, E.B. Olasz, K.E. Scott, H. Zaghoul, *Modified simulation of the urban radio propagation radio channel (SURP)*, IEE Electronics Letters, Vol. 29, No. 21, pages 1825-1826, October 1993.
- [49] H. Hashemi, *Simulation of the Urban Radio Propagation Channel*, IEEE Transactions on Vehicular Technology, Vol. 28, No. 3, pages 213-225, August 1979.
- [50] G.L. Turin, F.D. Clapp, T.L. Johnston, S.B. Fine, D. Laury, *A statistical model of urban multipath propagation*, IEEE Transactions on Vehicular Technology, Vol. 21, No. 1, pages 1-9, February 1972.
- [51] A.A.M. Saleh, R.A. Valenzuela, *A statistical model for indoor multipath propagation*, IEEE Journal on Selected Areas in Communication, Vol. 5, No. 2, pages 128-137, February 1987.

- [52] M. Petković, *Iterative Methods for Simultaneous Inclusion of Polynomial Zeros*, Springer-Verlag, 1989.
- [53] B. Davies, *IRIS Development System*, TR Labs internal document, April 1994.
- [54] *The Cellular Telecommunications Industry Association's Annualized Wireless Industry Data Survey Results*, on the web page of CTIA, [www.wow-com.com](http://www.wow-com.com).
- [55] F. Benner, *Method for Assigning Telecommunications Channels in a Cellular Telephone System*, U.S. Patent 5,111,534, May 1992.
- [56] S. Faruque, *The  $N = 9$  Frequency Plan: A modified Technique to Enhance C/I Performance and Capacity*, IEEE 2nd International Conference Proceedings on Universal Personal Communications, pages 718-722, 1993.
- [57] *EIA/TIA Standard, Mobile Station - Land Station Compatibility Specification*. EIA/TIA-533, September 1989.
- [58] R. Klukas, A. Borsodi, M. Astridge, M. Fattouche, G. Lachapelle, *A System to Position Analog Cellular Telephones*, Wireless 96, The 8<sup>th</sup> International Conference on Wireless Communications, pages 470-474, July 1996.
- [59] R. Klukas, G. Lachapelle, M. Fattouche, *Field Tests of a Cellular Telephone Positioning System*, IEEE Vehicular Technology Conference, pages 470-474, May 1997.
- [60] *TDMA Cellular/PCS - Radio Interface - Mobile Station - Base Station Compatibility - Digital Control Channel*, EIA/TIA/IS-136.1, Telecommunications Industry Association, September 1997.
- [61] J.S. Kaufman, *Analysis of the Random Access Channel in AMPS and IS-54 TDMA*, Wireless 96, July 1996.
- [62] T.S. Rappaport, S.Y. Seidel, R. Singh, *900 MHz Multipath Propagation Measurements for U.S. Digital Cellular Radiotelephone*, IEEE Transactions on Vehicular Technology, Vol. 39, No. 2, pages 132-139, May 1990.

- [63] E.S. Sousa, V.M. Jovanovic, C. Daigneault, *Delay Spread Measurements For The Digital Cellular Channel In Toronto*, Proceedings of The Third IEEE International Symposium on Personal, Indoor and Mobile Radio Communications, pages 80-85, October 1992.
- [64] N. Benner, Technical Planner, AGT Mobility. Private Communication, 1995.
- [65] N.A. D'Andrea, U. Mengali, *A Simulation Study of Clock Recovery in QPSK and 9QPRS Systems*, IEEE Transactions on Communications, Vol. 33, No. 10, pages 1139-1146, October 1985.
- [66] K.E. Scott, E.B. Olasz, *Simultaneous Clock Phase and Frequency Offset Estimation*, IEEE Transactions on Communications, Vol. 43, No. 7, pages 2263-2270, July 1995.
- [67] W.A. Gardner, C.M. Spooner, *Signal Interception: Performance Advantages of Cyclic-Feature Detectors*, IEEE Transactions on Communications, Vol. 40, No. 1, pages 149-159, January 1992.
- [68] M. Hata, *Empirical Formula for Propagation Loss in Land Mobile Radio Services*, IEEE Transactions on Vehicular Technology, Vol. 29, No. 3, pages 317-325, August 1980.
- [69] R.B. Carey, *Technical factors affecting the assignment of facilities in the domestic public land mobile radio service*, FCC report R-6406, June 1964.
- [70] J. Walfisch, H.L. Bertoni, *A Theoretical Model of UHF Propagation in Urban Environments*, IEEE Transactions on Antennas and Propagation, Vol. 36, No. 12, pages 1788-1796, December 1988.
- [71] Y. Okumura, E. Ohmori, T. Kawano, K. Fukuda, *Field strength and its variability in VHF and UHF land-mobile radio service*, Review of the Electronic Communications Laboratory, Vol. 16, No. 9, pages 825-873, 1968.
- [72] G.L. Turin, W.S. Jewell, T.L. Johnston, *Simulation of Urban Vehicle-Monitoring Systems*, IEEE Transactions on Vehicular Technology, Vol. 21, No. 1, pages 9-16, February 1972.

- [73] W.T. Warren, J.R. Whitten, R.E. Anderson, M.A. Merigo, *Vehicle Location System Experiment*, IEEE Transactions on Vehicular Technology, Vol. 21, No. 3, pages 92-101, August 1972.
- [74] H. Patram, Superintendent, The City of Calgary Fire Department. Private Communication, May 1997.
- [75] R.B. Bent, Celltrax Inc., *CTIA E911 Workshop on Location Technology*, Washington D.C., January 1997.
- [76] R. Klukas, Department of Geomatics Engineering, University of Calgary. Private Communication, April 1997.
- [77] *Mobile Station - Base Station Compatibility Standard for Dual Mode Wideband Spread Spectrum Cellular Systems*. TIA/EIA IS-95-B, August 1998.
- [78] E.O. Frye, *GPS Signal Availability in Land Mobile Applications*, Navigation: Journal of the Institute of Navigation, Vol. 36, No. 3, pages 287-301, Fall 1989.
- [79] T.E. Melgard, G. Lachapelle, H. Gehue, *GPS Signal Availability in an Urban Area – Receiver Performance Analysis*, IEEE International Conference on Position, Location, and Navigation, pages 487-493, 1994.
- [80] G. Lachapelle, B. Townsend, D. Halayko, *Analysis of GPS and LORAN-C Performance for Land Vehicle Navigation in the Canadian Rockies*, IEEE AES Magazine, Vol. 7, No. 5, pages 24-28, May 1992.
- [81] *Automatic Vehicle Monitoring Systems*, FCC Report and Order, Docket No. 95-41, February 1995.

## Appendix A: Overhead Messages

Table A.1. Station Class Mark

Power Class	SCM <sub>4,0</sub>	Transmission	SCM <sub>4,0</sub>	Bandwidth	SCM <sub>4,0</sub>
Class I	0XX00	continuous	XX0XX	20 MHz	X0XXX
Class II	0XX01	discontinuous	XX1XX	25 MHz	X1XXX
Class III	0XX10				
Class IV	0XX11				
Class V	1XX00				
Class VI	1XX01				
Class VII	1XX10				
Class VIII	1XX11				

Table A.2. Abbreviated Order and Order Qualification Codes

<u>Order Code</u>	<u>Order Qualification Code</u>	<u>Function</u>
00000	000	Page or Origination
00001	000	Alert
00011	000	Release
00100	000	Reorder
00110	000	Stop Alert
00111	000	Audit
01000	000	Send called address
01001	000	Intercept
01010	000	Maintenance
01011	000	Change to Power Level 0
01011	001	Change to Power Level 1
01011	010	Change to Power Level 2
01011	011	Change to Power Level 3
01011	100	Change to Power Level 4
01011	101	Change to Power Level 5
01011	110	Change to Power Level 6
01011	111	Change to Power Level 7
01100	000	Directed retry (not last try)
01100	001	Directed retry (last try)
01101	000	Non-autonomous Registration (Make whereabouts unknown)
01101	001	Non-autonomous Registration (Make whereabouts known)
01101	010	Autonomous Registration (Make whereabouts unknown)
01101	011	Autonomous Registration (Make whereabouts known)

Table A.3. Mobile Phone Class Identifier

<b>MPCI</b>	<b>Mobile Station Type</b>
00	EIA-553 or IS-54-A (analog)
01	EIA/TIA IS-54-B (dual-mode)
10	reserved
11	reserved