

ANALYSIS OF RADIO FREQUENCY INTERFERENCE
EFFECTS ON A MODERN COARSE ACQUISITION CODE
GLOBAL POSITIONING SYSTEM (GPS) RECEIVER

THESIS

Kenneth D. Johnston
Major, Canadian Forces

AFIT/GSO/ENG/99M-02

VOLUME 1

Approved for public release; distribution unlimited


DTIC QUALITY INSPECTED 2

19990409 114

ANALYSIS OF RADIO FREQUENCY INTERFERENCE EFFECTS
ON A MODERN COARSE ACQUISITION (C/A) CODE
GLOBAL POSITIONING SYSTEM (GPS) RECEIVER


Kenneth Dale Johnston, B.Sc.(Applied)
Major, Canadian Forces

Approved:



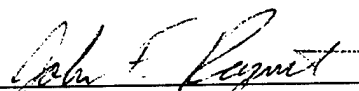
Major Mikel M. Miller, PhD
Assistant Professor, Thesis Advisor

4 Mar 99
Date



Lieutenant Colonel Stuart Kramer, PhD
Associate Professor, Thesis Committee

4 MAR 99
Date



Captain John Raquet, PhD
Assistant Professor, Thesis Committee

4 MAR 99
Date

The views expressed in this thesis are those of the author and do not reflect the official policy or position of the U.S. Department of Defense, the U.S. Government, the Canadian Department of Defence, or the Canadian Government.

AFIT/GSO/ENG/99M-02

**ANALYSIS OF RADIO FREQUENCY INTERFERENCE EFFECTS
ON A MODERN COARSE ACQUISITION (C/A) CODE
GLOBAL POSITIONING SYSTEM (GPS) RECEIVER**

VOLUME 1

THESIS

**Presented to the Faculty of the Graduate School of Engineering
of the Air Force Institute of Technology
Air University
In Partial Fulfillment of the
Requirements for the Degree of
Master of Science in Space Operations**

**Kenneth D. Johnston, B.Sc. (Applied)
Major, Canadian Forces**

March 1999

Approved for public release; distribution unlimited

ACKNOWLEDGEMENTS

I would like to begin by thanking AFIT/ENY and ENG faculties for allowing me to conduct research in the advanced technology area of jamming of GPS signals. The thesis research was personally very rewarding. My thanks to Lieutenant Colonel Stuart Kramer for his support of AFIT's Space Operations Program. I want to thank Major Mike Miller and Captain John Raquet for sharing their GPS expertise and providing support to complete my thesis research. I would also like to thank Mr. Don Smith for his excellent technical lab support. Don always would take the time to discuss technical issues, and to track down the necessary equipment.

My regards to fellow members of the MS Space Operations and MS Electrical Engineering in the Navigation and Controls Sequence for their sense of humor, hard work and dedication throughout my time at AFIT. I would also like to make special mention of Squadron Leader (RAAF) Ken Crowe and his family for sharing the AFIT experience.

I especially want to thank my daughters, Taylor and Ellen and my wife, Andy for their patience and understanding during my studies.

Finally, this work is dedicated to Major Wally Sweetman and Fred Fox, two old friends who remind me to live each day to the fullest.

Table of Contents

VOLUME 1

	Page
Acknowledgements	ii
List of Figures	vi
List of Tables	xii
Abstract.....	xiii
I. Introduction.....	1-1
1.1 Background	1-1
1.2 Problem Statement	1-4
1.3 Summary of Current Knowledge	1-5
1.4 Assumptions.....	1-8
1.5 Scope	1-8
1.6 Approach.....	1-9
1.7 Materials and Equipment.....	1-9
1.8 Thesis Organization.....	1-10
II. GPS Signal Characteristics	2-1
2.1 Chapter Overview.....	2-1
2.2 Initial Spread Spectrum Flux Density Requirements	2-1
2.3 GPS Signal Overview	2-2
2.4 Spectral Characteristics of C/A Code.....	2-4
2.5 Development of Interference Signal Characteristics.....	2-5
2.6 Receiver Tracking Loops.....	2-11
2.7 Doppler Shift.....	2-13
2.8 C/N_0 and J/S Calculations.....	2-14
2.9 Previous GPS Modeling and Simulation at AFIT	2-18
2.10 Chapter Summary.....	2-19
III. Equipment Configuration and Test Set-Up	3-1
3.1 Chapter Overview.....	3-1
3.2 Differential GPS (DGPS)	3-1
3.3 RTCM Message Formats.....	3-3
3.4 Equipment Configuration.....	3-4
3.5 Measurement of GPS and Jamming Signals	3-6
3.6 Jamming Scenarios.....	3-9
3.7 Chapter Summary.....	3-12

IV. Results and Analysis.....	4-1
4.1 Chapter Overview.....	4-1
4.2 Equipment Configuration.....	4-1
4.3 Jam to Signal Measurements.....	4-2
4.4 Test Results Overview.....	4-3
4.5 No Jamming Test Results.....	4-11
4.5.1 Test 1 Results (Figures Contained in Appendix I).....	4-11
4.5.2 Test 2 Results (Figures Contained in Appendix J).....	4-16
4.6 CW Jamming Test Results.....	4-21
4.6.1 Test 3 Results (Figures Contained in Appendix K).....	4-21
4.6.2 Test 4 Results (Figures Contained in Appendix L).....	4-25
4.6.3 Test 5 Results (Figures Contained in Appendix M).....	4-28
4.6.4 Test 6 Results (Figures Contained in Appendix N).....	4-30
4.6.5 Test 7 Results (Figures Contained in Appendix O).....	4-34
4.6.6 Test 8 Results (Figures Contained in Appendix P).....	4-37
4.7 Swept CW Test Results.....	4-39
4.7.1 Test 9 Results (Figures Contained in Appendix Q).....	4-40
4.7.2 Test 10 Results (Figures Contained in Appendix R).....	4-42
4.7.3 Test 11 Results (Figures Contained in Appendix S).....	4-45
4.8 CW Jamming Impact on Position Error.....	4-48
4.8.1 Test 12 Results (Figures Contained in Appendix T).....	4-48
4.9 Special Observations.....	4-51
4.9.1 Bias in Doppler Frequency Offset.....	4-52
4.9.2 Wave in Doppler Frequency Offset.....	4-54
4.9.3 Intermittent Loss of Lock on PRN 15.....	4-54
4.9.4 Multipath Effects.....	4-55
4.9.5 Jamming Using Strong Spectral Line Characteristics.....	4-55
4.10 Development of GPS Jamming Training.....	4-56
4.11 Chapter Summary.....	4-58
V. Summary, Conclusions and Recommendations.....	5-1
5.1 Summary.....	5-1
5.2 Conclusions.....	5-2
5.3 Recommendations.....	5-4
Bibliography.....	BIB-1
Vita.....	VIT-1

VOLUME 2

Appendix A 1988 Doppler Survey of AFIT Building 640 Rooftop.....	A-1
Appendix B Latitude/Longitude/Altitude to ECEF Transformations	B-1
Appendix C XR5-M Symbol Variables.....	C-1
Appendix D XR5-M Technical Information.....	D-1
Appendix E Hewlett Packard Equipment Description	E-1
Appendix F MATLAB® Software Code	F-1
Appendix G Sources of Interference to GPS Receivers & Mitigation Techniques	G-1
Appendix H Summary of Lessons Learned	H-1
Appendix I Test 1 Figures I.1-I.18.....	I-1
Appendix J Test 2 Figures J.1-J.18	J-1
Appendix K Test 3 Figures K.1-K.18.....	K-1
Appendix L Test 4 Figures L.1-L.18.....	L-1
Appendix M Test 5 Figures M.1-M.18.....	M-1
Appendix N Test 6 Figures N.1-N.18.....	N-1
Appendix O Test 7 Figures O.1-O.18.....	O-1
Appendix P Test 8 Figures P.1-P.19	P-1
Appendix Q Test 9 Figures Q.1-Q.20.....	Q-1
Appendix R Test 10 Figures R.1-R.18	R-1
Appendix S Test 11 Figures S.1-S.19	S-1
Appendix T Test 12 Figures T.1-T.22.....	T-1

List of Figures

Figure	Page
2.1 Combined Power Spectra of C/A and P(Y) code.....	2-4
2.2 Example Spectrum of Gold Code for Period P=1023	2-6
2.3 Generic Digital Receiver Tracking Channels.....	2-12
3.1 XR5-M Receiver.....	3-5
3.2 Equipment Test Configuration	3-7
4.1 Satellite Constellation 1555Z 20 Nov 98.....	4-3
4.2 PRN # Used in Navigation Solution versus Time	4-6
4.3 PRN # Assigned to Each Tracking Channel versus Time	4-6
4.4 GDOP versus Time.....	4-7
4.5 Doppler Frequency Offset versus Time.....	4-8
4.6 X, Y, Z, and 3D Error (meters) versus Time.....	4-9
4.7 XR5-M Receiver Clock Bias and Drift versus Time.....	4-9
4.8 C/N ₀ versus Time.....	4-10
I.1 GPS Satellites in View.....	I-1
I.2 GPS Satellites in View.....	I-2
I.3 PRN # Used In Navigation Solution.....	I-3
I.4 PRN # Assigned to Each Tracking Channel	I-4
I.5 GDOP.....	I-5
I.6 Doppler Frequency Offset.....	I-6
I.7 Doppler Frequency Offset.....	I-7
I.8 Doppler Frequency Offset.....	I-8
I.9 Doppler Frequency Offset.....	I-9
I.10 X,Y,Z and 3D Position Error	I-10
I.11 X,Y,Z and 3D Position Error	I-11
I.12 Receiver Clock Bias and Drift.....	I-12
I.13 C/N ₀ vs Time Channel 1 and Channel 2	I-13
I.14 C/N ₀ vs Time Channel 3 and Channel 4	I-14
I.15 C/N ₀ vs Time Channel 5 and Channel 6	I-15
I.16 C/N ₀ vs Time Channel 7 and Channel 8	I-16
I.17 C/N ₀ vs Time Channel 9 and Channel 10	I-17
I.18 C/N ₀ vs Time Channel 11 and Channel 12	I-18
J.1 GPS Satellites in View.....	J-1
J.2 GPS Satellites in View.....	J-2
J.3 PRN # Used In Navigation Solution.....	J-3
J.4 PRN # Assigned to Each Tracking Channel	J-4
J.5 GDOP.....	J-5
J.6 Doppler Frequency Offset.....	J-6
J.7 Doppler Frequency Offset.....	J-7
J.8 Doppler Frequency Offset.....	J-8

J.9	Doppler Frequency Offset.....	J-9
J.10	X,Y,Z and 3D Position Error	J-10
J.11	X,Y,Z and 3D Position Error	J-11
J.12	Receiver Clock Bias and Drift.....	J-12
J.13	C/N ₀ vs Time Channel 1 and Channel 2	J-13
J.14	C/N ₀ vs Time Channel 3 and Channel 4	J-14
J.15	C/N ₀ vs Time Channel 5 and Channel 6	J-15
J.16	C/N ₀ vs Time Channel 7 and Channel 8	J-16
J.17	C/N ₀ vs Time Channel 9 and Channel 10	J-17
J.18	C/N ₀ vs Time Channel 11 and Channel 12	J-18
K.1	GPS Satellites in View.....	K-1
K.2	GPS Satellites in View.....	K-2
K.3	PRN # Used In Navigation Solution.....	K-3
K.4	PRN # Assigned to Each Tracking Channel	K-4
K.5	GDOP.....	K-5
K.6	Doppler Frequency Offset.....	K-6
K.7	Doppler Frequency Offset.....	K-7
K.8	Doppler Frequency Offset.....	K-8
K.9	Doppler Frequency Offset.....	K-9
K.10	X,Y,Z and 3D Position Error	K-10
K.11	X,Y,Z and 3D Position Error	K-11
K.12	Receiver Clock Bias and Drift.....	K-12
K.13	C/N ₀ vs Time Channel 1 and Channel 2	K-13
K.14	C/N ₀ vs Time Channel 3 and Channel 4	K-14
K.15	C/N ₀ vs Time Channel 5 and Channel 6	K-15
K.16	C/N ₀ vs Time Channel 7 and Channel 8	K-16
K.17	C/N ₀ vs Time Channel 9 and Channel 10	K-17
K.18	C/N ₀ vs Time Channel 11 and Channel 12	K-18
L.1	GPS Satellites in View.....	L-1
L.2	GPS Satellites in View.....	L-2
L.3	PRN # Used In Navigation Solution.....	L-3
L.4	PRN # Assigned to Each Tracking Channel	L-4
L.5	GDOP.....	L-5
L.6	Doppler Frequency Offset.....	L-6
L.7	Doppler Frequency Offset.....	L-7
L.8	Doppler Frequency Offset.....	L-8
L.9	Doppler Frequency Offset.....	L-9
L.10	X,Y,Z and 3D Position Error	L-10
L.11	X,Y,Z and 3D Position Error	L-11
L.12	Receiver Clock Bias and Drift.....	L-12
L.13	C/N ₀ vs Time Channel 1 and Channel 2	L-13
L.14	C/N ₀ vs Time Channel 3 and Channel 4	L-14
L.15	C/N ₀ vs Time Channel 5 and Channel 6	L-15
L.16	C/N ₀ vs Time Channel 7 and Channel 8	L-16
L.17	C/N ₀ vs Time Channel 9 and Channel 10	L-17

L.18	C/N ₀ vs Time Channel 11 and Channel 12	L-18
M.1	GPS Satellites in View	M-1
M.2	GPS Satellites in View	M-2
M.3	PRN # Used In Navigation Solution.....	M-3
M.4	PRN # Assigned to Each Tracking Channel	M-4
M.5	GDOP.....	M-5
M.6	Doppler Frequency Offset.....	M-6
M.7	Doppler Frequency Offset.....	M-7
M.8	Doppler Frequency Offset.....	M-8
M.9	Doppler Frequency Offset.....	M-9
M.10	X,Y,Z and 3D Position Error	M-10
M.11	X,Y,Z and 3D Position Error	M-11
M.12	Receiver Clock Bias and Drift.....	M-12
M.13	C/N ₀ vs Time Channel 1 and Channel 2	M-13
M.14	C/N ₀ vs Time Channel 3 and Channel 4	M-14
M.15	C/N ₀ vs Time Channel 5 and Channel 6	M-15
M.16	C/N ₀ vs Time Channel 7 and Channel 8	M-16
M.17	C/N ₀ vs Time Channel 9 and Channel 10	M-17
M.18	C/N ₀ vs Time Channel 11 and Channel 12	M-18
N.1	GPS Satellites in View	N-1
N.2	GPS Satellites in View	N-2
N.3	PRN # Used In Navigation Solution.....	N-3
N.4	PRN # Assigned to Each Tracking Channel	N-4
N.5	GDOP.....	N-5
N.6	Doppler Frequency Offset.....	N-6
N.7	Doppler Frequency Offset.....	N-7
N.8	Doppler Frequency Offset.....	N-8
N.9	Doppler Frequency Offset.....	N-9
N.10	X,Y,Z and 3D Position Error	N-10
N.11	X,Y,Z and 3D Position Error	N-11
N.12	Receiver Clock Bias and Drift.....	N-12
N.13	C/N ₀ vs Time Channel 1 and Channel 2	N-13
N.14	C/N ₀ vs Time Channel 3 and Channel 4	N-14
N.15	C/N ₀ vs Time Channel 5 and Channel 6	N-15
N.16	C/N ₀ vs Time Channel 7 and Channel 8	N-16
N.17	C/N ₀ vs Time Channel 9 and Channel 10	N-17
N.18	C/N ₀ vs Time Channel 11 and Channel 12	N-18
O.1	GPS Satellites in View	O-1
O.2	GPS Satellites in View	O-2
O.3	PRN # Used In Navigation Solution.....	O-3
O.4	PRN # Assigned to Each Tracking Channel	O-4
O.5	GDOP.....	O-5
O.6	Doppler Frequency Offset.....	O-6
O.7	Doppler Frequency Offset.....	O-7

O.8	Doppler Frequency Offset.....	O-8
O.9	X,Y,Z and 3D Position Error	O-9
O.10	X,Y,Z and 3D Position Error	O-10
O.11	Receiver Clock Bias and Drift.....	O-11
O.12	C/N ₀ vs Time Channel 1 and Channel 2	O-12
O.13	C/N ₀ vs Time Channel 3 and Channel 4	O-13
O.14	C/N ₀ vs Time Channel 5 and Channel 6	O-14
O.15	C/N ₀ vs Time Channel 7 and Channel 8	O-15
O.16	C/N ₀ vs Time Channel 9 and Channel 10	O-16
O.17	C/N ₀ vs Time Channel 11 and Channel 12	O-17
O.18	Jamming Level J/S vs Time	O-18
P.1	GPS Satellites in View.....	P-1
P.2	GPS Satellites in View.....	P-2
P.3	PRN # Used In Navigation Solution.....	P-3
P.4	PRN # Assigned to Each Tracking Channel	P-4
P.5	GDOP.....	P-5
P.6	Doppler Frequency Offset.....	P-6
P.7	Doppler Frequency Offset.....	P-7
P.8	Doppler Frequency Offset.....	P-8
P.9	Doppler Frequency Offset.....	P-9
P.10	X,Y,Z and 3D Position Error	P-10
P.11	X,Y,Z and 3D Position Error	P-11
P.12	Receiver Clock Bias and Drift.....	P-12
P.13	C/N ₀ vs Time Channel 1 and Channel 2	P-13
P.14	C/N ₀ vs Time Channel 3 and Channel 4	P-14
P.15	C/N ₀ vs Time Channel 5 and Channel 6	P-15
P.16	C/N ₀ vs Time Channel 7 and Channel 8	P-16
P.17	C/N ₀ vs Time Channel 9 and Channel 10	P-17
P.18	C/N ₀ vs Time Channel 11 and Channel 12	P-18
P.19	Jamming Level J/S vs Time	P-19
Q.1	GPS Satellites in View.....	Q-1
Q.2	GPS Satellites in View.....	Q-2
Q.3	PRN # Used In Navigation Solution.....	Q-3
Q.4	PRN # Assigned to Each Tracking Channel	Q-4
Q.5	GDOP.....	Q-5
Q.6	Doppler Frequency Offset.....	Q-6
Q.7	Doppler Frequency Offset.....	Q-7
Q.8	Doppler Frequency Offset.....	Q-8
Q.9	Doppler Frequency Offset.....	Q-9
Q.10	X,Y,Z and 3D Position Error	Q-10
Q.11	X,Y,Z and 3D Position Error	Q-11
Q.12	X,Y,Z and 3D Position Error	Q-12
Q.13	Receiver Clock Bias and Drift.....	Q-13
Q.14	C/N ₀ vs Time Channel 1 and Channel 2	Q-14
Q.15	C/N ₀ vs Time Channel 3 and Channel 4	Q-15

Q.16	C/N ₀ vs Time Channel 5 and Channel 6	Q-16
Q.17	C/N ₀ vs Time Channel 7 and Channel 8	Q-17
Q.18	C/N ₀ vs Time Channel 9 and Channel 10	Q-18
Q.19	C/N ₀ vs Time Channel 11 and Channel 12	Q-19
Q.20	Jamming Level J/S vs Time	Q-20
R.1	GPS Satellites in View.....	R-1
R.2	GPS Satellites in View.....	R-2
R.3	PRN # Used In Navigation Solution.....	R-3
R.4	PRN # Assigned to Each Tracking Channel	R-4
R.5	GDOP.....	R-5
R.6	Doppler Frequency Offset.....	R-6
R.7	Doppler Frequency Offset.....	R-7
R.8	Doppler Frequency Offset.....	R-8
R.9	X,Y,Z and 3D Position Error	R-9
R.10	X,Y,Z and 3D Position Error	R-10
R.11	Receiver Clock Bias and Drift.....	R-11
R.12	C/N ₀ vs Time Channel 1 and Channel 2	R-12
R.13	C/N ₀ vs Time Channel 3 and Channel 4	R-13
R.14	C/N ₀ vs Time Channel 5 and Channel 6	R-14
R.15	C/N ₀ vs Time Channel 7 and Channel 8	R-15
R.16	C/N ₀ vs Time Channel 9 and Channel 10	R-16
R.17	C/N ₀ vs Time Channel 11 and Channel 12	R-17
R.18	Jamming Level J/S vs Time	R-18
S.1	GPS Satellites in View.....	S-1
S.2	GPS Satellites in View.....	S-2
S.3	PRN # Used In Navigation Solution.....	S-3
S.4	PRN # Assigned to Each Tracking Channel	S-4
S.5	GDOP.....	S-5
S.6	Doppler Frequency Offset.....	S-6
S.7	Doppler Frequency Offset.....	S-7
S.8	Doppler Frequency Offset.....	S-8
S.9	Doppler Frequency Offset.....	S-9
S.10	X,Y,Z and 3D Position Error	S-10
S.11	X,Y,Z and 3D Position Error	S-11
S.12	Receiver Clock Bias and Drift.....	S-12
S.13	C/N ₀ vs Time Channel 1 and Channel 2	S-13
S.14	C/N ₀ vs Time Channel 3 and Channel 4	S-14
S.15	C/N ₀ vs Time Channel 5 and Channel 6	S-15
S.16	C/N ₀ vs Time Channel 7 and Channel 8	S-16
S.17	C/N ₀ vs Time Channel 9 and Channel 10	S-17
S.18	C/N ₀ vs Time Channel 11 and Channel 12	S-18
S.19	Jamming Level J/S vs Time	S-19

T.1	GPS Satellites in View.....	T-1
T.2	GPS Satellites in View.....	T-2
T.3	PRN # Used In Navigation Solution.....	T-3
T.4	PRN # Assigned to Each Tracking Channel	T-4
T.5	GDOP.....	T-5
T.6	Doppler Frequency Offset.....	T-6
T.7	Doppler Frequency Offset.....	T-7
T.8	Doppler Frequency Offset.....	T-8
T.9	Doppler Frequency Offset.....	T-9
T.10	Receiver Fix Status.....	T-10
T.11	X,Y,Z and 3D Position Error	T-11
T.12	X,Y,Z and 3D Position Error	T-12
T.13	X,Y,Z and 3D Position Error	T-13
T.14	X,Y,Z and 3D Position Error	T-14
T.15	Receiver Clock Bias and Drift.....	T-15
T.16	C/N ₀ vs Time Channel 1 and Channel 2	T-16
T.17	C/N ₀ vs Time Channel 3 and Channel 4	T-17
T.18	C/N ₀ vs Time Channel 5 and Channel 6	T-18
T.19	C/N ₀ vs Time Channel 7 and Channel 8	T-19
T.20	C/N ₀ vs Time Channel 9 and Channel 10	T-20
T.21	C/N ₀ vs Time Channel 11 and Channel 12	T-21
T.22	Jamming Level J/S vs Time	T-22

List of Tables

Table	Page
1.1 Summary of Appendices	1-11
3.1 No Jamming Tests	3-10
3.2 CW Jamming Tests	3-11
3.3 Swept CW Jamming Tests	3-12
3.4 CW Jamming Position Error Measurements	3-12
4.1 J/S Calculations	4-2
4.2 Summary of Test Parameters	4-4
4.3 PRN Number Assigned to Receiver Tracking Channel	4-12
4.4 PRN Doppler Frequency Offset Intercepts	4-20
4.5 Position Error as a Result of CW Jamming	4-52
4.6 Summary of No Jamming Results for Tests 1 and 2	4-59

Abstract

The purpose of this thesis was to investigate the performance of a twelve channel Standard Positioning Service (SPS) based Global Positioning System (GPS) receiver using an eight state Kalman filter in a hostile radio frequency (RF) environment and to develop instructional tools for teaching RF interference on GPS receivers. The two types of jamming signals generated included Continuous Wave (CW) and Swept CW. Actual GPS and jamming signals were used in the research.

The signals received from GPS satellites exhibit a Doppler shift which vary between approximately \pm six Kilohertz. The Doppler shift frequency can be reasonably predicted for a given time of day, for a given satellite, and for a known receiver location using GPS satellite almanac or ephemeris data. Additionally, the Pseudorandom Noise (PRN) Coarse Acquisition (C/A) code for each satellite exhibits specific maximum amplitude spectral lines. By tailoring the jamming signals to match with the Doppler shifted satellite frequencies and offsetting the jamming to a maximum spectral line, it was shown that individual Navstar XR5-M receiver channels for specific satellites could be selectively jammed/spoofed.

Swept CW jamming resulted in pulling the XR5-M receiver tracking channels off frequency by up to 20 Kilohertz but resulted in a maximum position error of only 220 meters. The CW jamming of at least one of the XR5-M receiver channels resulted in position errors in the receiver in excess of 12 kilometers.

***ANALYSIS OF RADIO FREQUENCY INTERFERENCE EFFECTS
ON A MODERN COARSE ACQUISITION CODE (C/A)
GLOBAL POSITIONING SYSTEM (GPS) RECEIVER***

1. INTRODUCTION

1.1 BACKGROUND

In 1973 the United States (US) military formed a Joint Program Office (JPO) to address the proliferation of navigation systems in the US Armed Forces and to develop precision weapon delivery systems. The desired solution was to be a common system that could provide worldwide coverage and be useable by all NATO military services. The result was a ground-controlled spaced-based system known as the NAVSTAR Global Positioning System (GPS).

Recently a great deal of interest has resulted from potential loss or degradation of GPS signals due to Radio Frequency (RF) Interference (RFI). This thesis will investigate the effects of jamming GPS satellite signals received by a Standard Positioning Service (SPS) Coarse Acquisition (C/A) code based receiver.

The GPS satellite constellation consists of 24 satellites in six orbital planes with four satellites per plane at an altitude of 20,183.6 km in approximately 12 hour, nearly circular orbits with an inclination of 55 degrees from the equatorial plane. On the earth are five monitor stations used to track and upload the satellites with the most recent

navigational information regarding the constellation. The system received Initial Operational Capability (IOC) status on December 8, 1993. While the system was originally developed for the military, the applications for GPS have exploded in the civil markets. The popularity of the system has resulted in handheld receivers now costing less than \$100 US. More recently, there has been a great deal of interest in aircraft traffic control systems using GPS known as Wide Area Augmentation System (WAAS) and Local Area Augmentation System (LAAS) [PAR96].

The GPS system was originally designed to meet military needs; however, enormous growth in the civil sector has led to many innovative uses of GPS. Originally the system was to provide the military a more accurate three dimensional navigation solution accuracy of 16 meters spherical error probable (SEP) while civil users could expect a somewhat degraded position error solution of 100 meters (2DRMS). Signal processing developments and multi-receiver implementations have provided civil users with centimeter accuracy. As the civil sector continues to become more dependent on the GPS signals, there has been a desire for increased accuracy and robustness. In order to achieve improved accuracy and robustness, there has been a growing interest in sources of interference to the GPS signals.

Although the military operates GPS receivers which are reported to be jam resistant, a 1998 incident with the Air Force Research Laboratory (AFRL) Information Directorate facility at Griffis AFB, New York raised serious concerns about the use of stand-alone GPS in civil aviation. The lab had been conducting a test with a five watt transmitter and inadvertently left the system transmitting in the civil GPS

frequency band over a ten day period. The incident resulted in at least 16 different reports to the FAA from civilian aviators including a Continental Airlines flight. The FAA declared an interference zone of 300 kilometers until they investigated the problem and advised the Research Laboratory [GWM98].

The "New Scientist" article of 10 January 1998, stated that a Russian company called "Aviaconversia" was offering a four watt GPS/GLONASS jammer for under \$4000 US at the September 1997 Moscow Air Show. The article claimed that the jammer was capable of preventing civilian aircraft from locking on to GPS signals over a 200 km radius [SEI98].

The combination of the incident at the AFRL and the GPS jamming equipment at the 1997 Moscow Air Show sparked interest into the GPS jamming effects on civil aviation. The potential chaos created by a simple four watt transmitter on a solely GPS-based air traffic control system has raised some doubt about the current plans to phase out many ground based navigation systems. In particular, the US Congress recently expressed reluctance to phase out a ground-based system known as Loran. The US Congress expressed concern over the findings of the US Presidential Commission on Critical Infrastructure Protection that reported sole reliance on satellites for aviation could be hazardous. After reviewing the Department of Transport's (DoT) 1999 budget proposal, the US Congress directed the DoT to provide funds to operate Loran system as a backup to GPS until at least 2008 [PRI99].

In a hostile RF environment, a jammer signal could be used to either degrade or completely deny the use of the GPS signals. The GPS signal structure and forms of RF interference are discussed in further detail in Chapter 2.

1.2 PROBLEM STATEMENT

The US government funded and developed GPS primarily as a military system; however, there has been exponential growth worldwide in civilian applications. Even though the US government has provided assurances that the GPS signals would remain on during time of conflict [DOD97], US defense forces require the ability to deny an adversary the use of GPS. In future conflicts US forces will be required to deny an adversary's use of GPS by local area jamming and spoofing of the GPS signals. US universities and research and development organizations have been conducting GPS jamming trials for several years; however, detailed results of these trials are generally classified and are not available to foreign military.

The Canadian Forces (CF) currently operates a mixed fleet of military aircraft, in some cases using only C/A code receivers such as the Trimble Trimpack receiver in the CF Sea King (H3) helicopter. Shrinking Canadian defense budgets have raised questions regarding the military requirements for P(Y) code receivers and the associated costly antenna systems if the position and velocity accuracy of off-the-shelf C/A Code receivers with simple integration to other systems may suffice. Additionally, in future conflicts, it will be necessary for the Canadian Forces to maintain a war fighting capability while at the same time denying an adversary the use of GPS signals, thus a

jam resistant system will be critical to ensure adequate GPS availability. Interoperability with US forces will remain essential.

The loss of position, velocity, and an accurate timing reference due to interference to GPS signals is a major concern to the Canadian Forces. The sponsor for this research effort, the Canadian Forces School of Aerospace Studies (CFSAS) at Canadian Forces Base (CFB) Winnipeg, Manitoba, Canada, requested thesis research to be conducted in the field of Navigation Warfare (NavWar). This thesis research provides an insight into effective techniques for jamming a C/A code receiver at the unclassified level and means to mitigate these effects.

1.3 SUMMARY OF CURRENT KNOWLEDGE

Two leading textbooks on GPS [PAR96, KAP96] provide an excellent introduction into understanding GPS signal structure and RF interference effects on GPS. In particular Chapters 4, 5, and 6 of [KAP96] written by Mr. Phillip Ward, were used extensively in developing Chapter 2 of this thesis. Previous research into the jamming of GPS is highlighted in this section.

The Naval Air Warfare Center (NAWC) Weapons Division at China Lake has developed a limited number of small soda-can size GPS jammers. Based on discussions with NAWC staff, the basic characteristics are as follows: the unit operates at 200 milliwatts and has a RS232 port on the bottom allowing it to be programmed to generate various jamming signals. The unit should be positioned upright for jamming signals to be effective. Follow-on research is planned to investigate the ability to air

launch the units with a retarding system and for the units to be remotely programmed [NAW98].

The NAWC Weapons GPS/INS Section Navigation Laboratory has developed a GPS Receiver and Integration Test Facility using a IEC SCS2400 GPS Satellite Constellation Simulator, a STel 7200 GPS Satellite Signal Simulator, and a NavLab GPS Jammer System. Up to four jammers per L1 and L2 may be generated with variable power levels from 20 to 80 dB J/S over the full GPS spectrum including narrow-band, continuous waveform, pulsed, and narrow-band and wide-band with pseudo-random Gaussian distributed noise sequences. National Instruments Labview™ software is used extensively in the user interface design [BOG97, RAS97].

The NavWar Advanced Concept Technology Demonstrations (ACTD) program was funded for up to \$55M to be completed in FY99 to demonstrate NavWar protection and prevention technologies. Under this program electronic warfare enhancements are being developed and implemented on the Miniaturized Airborne GPS Receiver (MAGR), Embedded GPS/INS (EGI), and the handheld Precision Lightweight GPS Receiver (PLGR) [WWW1].

At least two companies are now marketing commercial products used to reduce the effects of RF interference to GPS receivers; Electro-Radiation Inc (ERI) of Fairfield, New Jersey, and Mayflower Communications Co from Billerica, MA. The Interference Suppression Unit (ISU), marketed by ERI, was combined with a MAGR and tested in May 1997 at Holloman AFB [BRAROS98, BRASNY98]. The flight testing, at White Sands Missile Range, was composed of five surface, high power, Right

Hand Circularly Polarized (RHCP), wide-band noise jammers and one airborne, RHCP, wide-band noise jammer. Results indicated that the ISU provides more than 20 dB of broadband noise margin [BRAROS98]. Electro-Radiation reports that the ISU also provides greater than 35 dB of narrow-band interference noise margin while maintaining code and carrier tracking.

Mayflower Communications has designed the AIC-2100 to reduce pulsed, CW and narrow-band interference and jamming by an improvement of up to 50 dB [UPT98]. A digital temporal filter is effective against narrow-band interference while antenna spatial filter techniques are effective against both narrow-band and wide-band sources of RFI. The AIC-2100 is designed to be operated at RF and would be a potential quick fix to mitigate narrow-band types of jamming; however, antenna beam-forming would still be required to suppress broadband sources of jamming [WWW2].

A presentation at the Institute of Navigation (ION) GPS Conference in September, 1998 in Nashville, Tennessee, highlighted research into direct Y code acquisition [ROU98]. A P(Y)-code receiver normally requires the Hand Over Word (HOW) from the C/A code to get P(Y) code lock. This presents an inherent vulnerability to a P(Y)-code receiver while in acquisition mode if the C/A code is being jammed and is therefore unable to get lock on the P(Y)-code. Not surprisingly, direct access to the encrypted P(Y) code for military users is one of the key elements of future "enhanced GPS" requirements passed into law by President Clinton in 1998 [ION98].

A potential wartime scenario would likely consist of US forces "carpet jamming" an entire area, thus negating the effective use of most C/A code receivers.

This scenario is reasonable provided direct P(Y) code acquisition is obtainable. The papers presented at ION-98 Conference highlighted that the hardware has been designed to meet these requirements [ROU98, WOL98].

1.4 ASSUMPTIONS

The thesis assumes that the performance of the Navstar XR5-M Receiver is typical of a C/A code receiver of mid 1990s technology. The Defense Mapping Agency 1988 survey of the AFIT Building 640 rooftop was assumed to be still valid.

1.5 SCOPE

The thesis investigates the theoretical and actual performance figures for a commercial-off-the-shelf (COTS) 12 channel Navstar XR5-M receiver in the presence of interference sources, specifically CW and swept CW signals. Actual data was first collected for the Navstar XR5-M receiver without jamming in order to establish baseline performance of the receiver. Performance of the XR5-M Receiver in the presence of actual interference signals was then measured. The primary area of research was the investigation of selectively jamming/spoofing an individual satellite signal at the GPS receiver using CW and swept CW signals, prior knowledge of a satellite's pseudorandom noise code, and the Doppler shift of the satellite signals. A comparison of position error as a result of CW and swept CW was also conducted.

1.6 APPROACH

Previous thesis work in the area of jamming of GPS signals at the US Air Force Institute of Technology (AFIT) made use of modeling and simulations. This thesis will present an analysis of actual GPS signals in the presence of real interference sources. A secondary goal of the thesis was to demonstrate RFI effects on GPS as part of the Advanced GPS Course taught by the Electrical Engineering Department at AFIT and as part of the course curriculum taught at the Canadian Forces School of Aerospace Studies at Winnipeg, Manitoba, Canada. Several jamming scenarios were investigated within funding limitations and available equipment at the time of the research.

1.7 MATERIALS AND EQUIPMENT

The main hardware components were two Navstar XR5-M 12 Channel GPS Receivers used in conjunction with Navstar software version 3.7 on two 486 Personal Computers (PC); the first receiver was used as a Base Station and the second was used as a mobile receiver. The PC computer display was used to control the receiver setups, configuration and for capturing XR5-M GPS data to file. The two Navstar receivers were used in a differential/relative GPS mode. Two Navstar GPS volute antennas with built in pre-amps were located on the AFIT Building 640 rooftop. An older Hewlett Packard (HP) spectrum analyzer was first used but did not provide accurate enough measurement of the signal generator output. The second HP spectrum analyzer was acceptable but initial testing using two Wavetek signal generators revealed that the Wavetek equipment was unsuitable due to frequency instability at GPS L1 frequencies.

The jamming hardware was finally achieved using an HP signal generator, an HP spectrum analyzer, and an HP variable attenuator. All jamming equipment was located in the Navigation/Controls Laboratory, Room 133 Building 640, Air Force Institute of Technology, Wright-Patterson Air Force Base, Ohio. The Mathworks™ Software MATLAB® version 5.2 was used on a Macintosh™ PowerPC® and a 400 MHz Pentium® II PC platform for the analysis of data output by the XR5-M receivers and for the preparation of the final thesis.

1.8 THESIS ORGANIZATION

Chapter 2 presents background information about the GPS signal, and an analysis of interference to GPS receivers. Chapter 3 provides a detailed description of the laboratory equipment setup of the two Navstar XR5-M receivers in the presence of CW jamming signals. A detailed analysis of the test results is provided in Chapter 4 while Chapter 5 offers conclusions and recommendations for future research. Table 1.1 provides a synopsis of material included in Appendix A to T.

Appendix A	1988 Doppler Survey of AFIT Building 640 Rooftop
Appendix B	Latitude/Longitude/Altitude to Earth Centered Earth Fixed (ECEF) Coordinates Transformation
Appendix C	XR5-M Receiver Symbol Variables
Appendix D	XR5-M Receiver Technical Information
Appendix E	Hewlett Packard Equipment Description
Appendix F	MATLAB [®] Software Code
Appendix G	Sources of RF Interference and Mitigation Techniques
Appendix H	Summary of Lessons Learned
Appendix I-T	Figures for Results of Tests 1 to 12 (to be read in conjunction with the analysis of results in Chapter 4)

Table 1.1 - Summary of Appendices

II. GPS SIGNAL CHARACTERISTICS

2.1 CHAPTER OVERVIEW

This chapter provides background information about the GPS signal characteristics, Doppler frequency offset and the development of GPS jamming requirements. Twelve GPS jamming scenarios, provided in Chapter 3, were developed to investigate RFI effects on the XR5-M receiver.

2.2 INITIAL SPREAD SPECTRUM FLUX DENSITY REQUIREMENTS

The basis for spread spectrum signals may be traced back to the original requirements for the GPS signals. It was essential that the GPS signals, especially from satellites at low elevation angles, would not interfere with land-based microwave communications. Typically a microwave station relays a large number of 4 kHz voice channels. Since GPS satellites can be seen low on the horizon it is likely that GPS signals would be in the field of view of the microwave stations. The International Telecommunication Union set the flux density for satellite-to-earth in the 1.525-2.500 GHz band for low elevation angles at a maximum of -154 dBw/m^2 for any 4 kHz band [PAR96]. This constraint is not on total radiated power but rather on power flux spectral density. This led to the development of spread spectrum signals where the signal is spread out over a wide bandwidth.

2.3 GPS SIGNAL OVERVIEW

The GPS satellites transmit continuously on two frequencies. The carrier frequencies are modulated with spread spectrum code with a unique pseudo-random noise sequence for each satellite PRN code at a particular chipping rate. This signal is also modulated with the 50 Hz navigation data message. One of the key differences between the Russian Global Navigation Satellite System (GLONASS) and GPS is that GLONASS uses different frequencies (Frequency Division Multiple Access) but transmits the same PRN code pair for each satellite. The GPS signal modulation is based on each satellite using a different PRN code but with the same code chipping rates and carrier frequencies. The GPS format is known as Code Division Multiple Access (CDMA).

The GPS signal structure is Direct-Sequence Spread Spectrum (DS/SS) which spreads the signal energy over a wide bandwidth. The primary frequency, known as L1, is at 1575.42 MHz. The coarse acquisition (C/A) code is a unique Gold code with a period of 1023 chips and is transmitted at a rate of 1.023×10^6 chips per second (cps) resulting in a code period of 1 millisecond (ms). The precision (P) code is transmitted at a rate of 10.23×10^6 cps and has a code period of one week.

Both the P and C/A code are published in ICD-GPS-200. The anti-spoof (AS) mode of operation known as Y code is an encrypted version of the P code. Because both the P code and Y code have the same chipping rate the acronym P(Y) code is commonly used.

Selective availability (SA) refers to the intentional degradation of the GPS satellite signal either by a pseudo-random dither of the satellite GPS clock frequency, or by incorporating small errors into the ephemeris information broadcast in the navigation message. SA denies full position and velocity accuracy to unauthorized users. Normally both AS and SA are enabled with exceptions occurring for testing purposes. Differential techniques as discussed in Chapter 3 were used to eliminate SA effects during data capture for this thesis research.

The combined power spectra of the C/A code and the P(Y) code are centered at the L1 frequency as shown in Figure 2.1. The first nulls of the C/A code are at ± 1.023 MHz from the center frequency and the first nulls of the P(Y) code power spectrum are at ± 10.23 MHz from the center frequency. The second frequency, L2, is centered at 1227.6 MHz. Normally, the L2 frequency is transmitted with P(Y) code power spectrum plus the 50 Hz navigation data Phase Shift Keyed (PSK) modulated onto the L2 carrier. The C/A code modulation is not normally transmitted on L2. This has been the subject of much discussion lately as the US government has agreed to provide a dedicated second civilian frequency at L2 starting with the first block IIF satellite [DIV99]. The primary role of the second frequency is to allow corrections for ionospheric errors. Additionally, a frequency of 1381.05 MHz, known as L3, is part of the Nuclear Detection system carried on board the GPS satellites [PAR96].

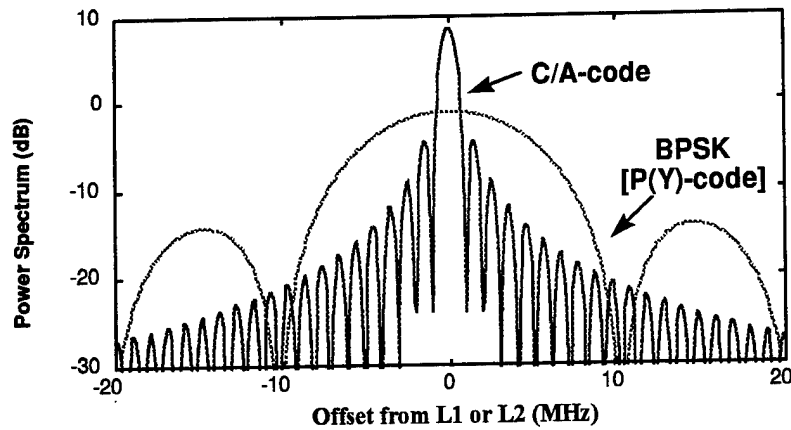


Figure 2.1 Combined Power Spectra of the C/A and P(Y) Code [AND98]

2.4 SPECTRAL CHARACTERISTICS OF C/A CODE

The development of the equations for the GPS signal architecture and interference signals were based on the work of Mr. Phillip Ward and Mr. A.J. Van Dierendonck [KAP96, PAR96]. The physical application of the auto-correlation function is used to achieve lock on the pseudo-random code. The auto-correlation function of the GPS C/A code is

$$R_G(\tau) = \frac{1}{1,023T_{CA}} \int_{t=0}^{t=1023} G_i(t)G_i(t + \tau)dt \quad (2-1)$$

where

- $G_i(t)$ = C/A code Gold code sequence as a function of time t for SV_i
- T_{CA} = C/A code chipping period (977.5 nsec)
- τ = phase of the time shift in the auto-correlation function

A special set of pseudo-range sequences with relatively low cross correlation properties is used for the C/A codes, this set is known as the Gold codes. The auto-correlation function of the C/A code is a series of correlation triangles with a period of 1,023 C/A code chips (or 1 msec). This explains why the C/A codes do not have a continuous power spectrum but instead have a 1000 Hz spaced line spectrum (separated by the inverse of the code period) as shown in Figure 2.2.

For the C/A code, small correlations occur in the intervals between the maximum correlation intervals. Fluctuations in the auto-correlation function results in a deviation from the line spectrum of the expected sinc $(\sin x/x)^2$ envelope. The ratio of the power in each C/A line to the total power fluctuates (nearly 8 dB) with respect to the -30 dB levels that would occur if every line contained the same power. Each of the C/A codes has certain "strong" lines (above the sinc envelope), an inherent weakness which continuous wave (CW) interference at this line frequency can attack as shown in Figure 2.2. Normally the correlation process of a CW line and a PRN code will spread the CW line, but the mixing process at certain "strong" C/A code line results in the RF interference line being suppressed less than at other frequencies. The net result is that CW energy can "leak" through the correlation process at this strong line [KAP96, PAR96].

2.5 DEVELOPMENT OF INTERFERENCE SIGNAL CHARACTERISTICS

A variety of RF signals may be used to interfere with the GPS signals at a receiver. Typically RF jamming can be of the form of CW, narrowband, and wideband

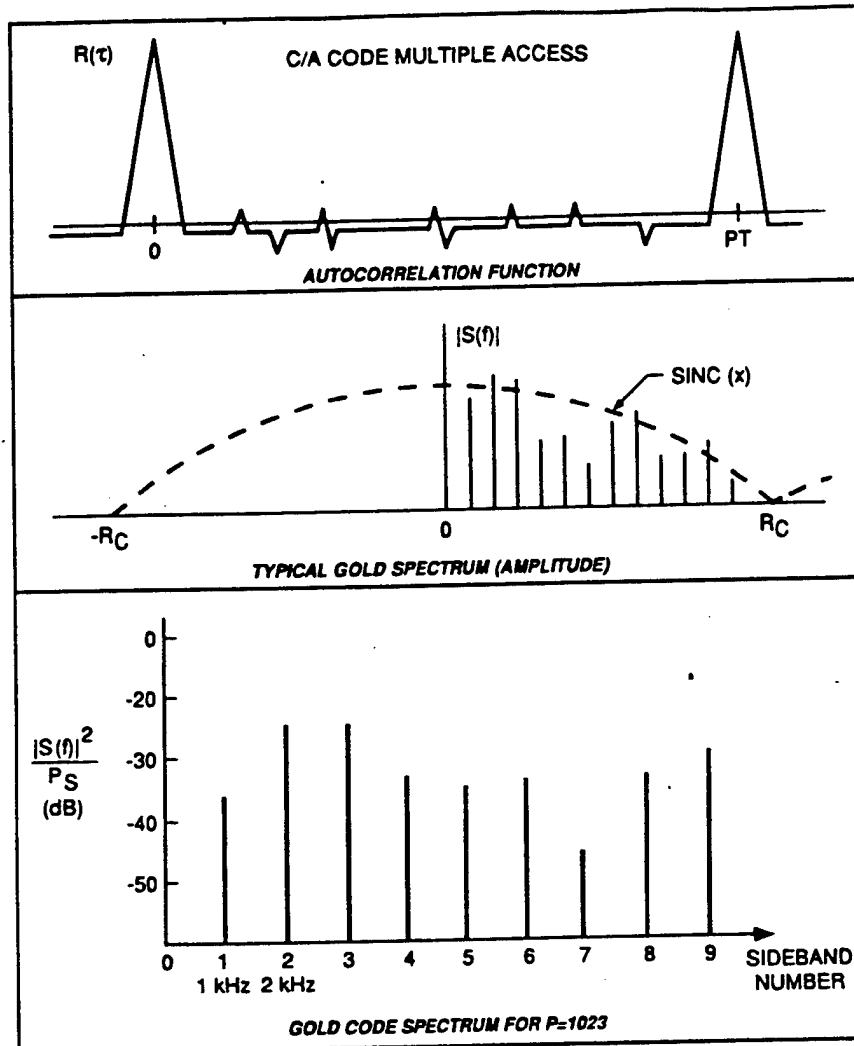


Figure 2.2 Example Spectrum of Gold Code for Period P=1023

electronic noise. Various forms of modulation of the carrier signal are available but the CW signal is probably the simplest form of interference. The signal is concentrated in a very narrow band around the L1 or L2 frequencies. More sophisticated methods involve the generation of replica PRN codes, and false data modulation.

The primary intent of jamming is to deny an adversary the use of the GPS signals. Spoofing on the other hand is the deliberate attempt to mimic the GPS signals; the results are incorrect position and velocity information. Effective spoofing could prevent a solely GPS-based weapon system from achieving the correct target location. The most challenging demands of spoofing require the target vehicle to be tracked with a radar or laser. Once the vehicle's track is determined, false signals can be generated which initially look very similar to the actual satellite's signals. Over a period of time the signals are modified such that the position and velocity is "walked-off" from the correct values.

The effects of ground based jamming and spoofing can be reduced by employing a directional antenna which can be nulled either from jamming sources, or optimized for the direction of actual satellite vehicles. Historically these types of antenna systems are larger, heavier, more complex, and more expensive. Other techniques apply pre-correlation and post-correlation signal processing techniques. Methods of reducing RFI to GPS receivers are discussed in further detail in Appendix G.

Signals which are received from satellites at low elevation angles are inherently more vulnerable to jamming. A simple method of RFI rejection may be to increase the

elevation mask angle for satellites low on the horizon. This technique was investigated in Test 8 of this thesis and the results are discussed in Section 4.6.6.

The GPS signal powers are specified in ICD-GPS 200 and are based on the use of a standard linearly polarized antenna. The minimum received power is specified at L1 for the C/A code as -160 dBw, for the L1 P(Y) code as -163 dBw, and for the L2 P(Y) code as -166 dBw. These figures should be adjusted by approximately 0.4 dB since GPS uses right hand circularly polarized (RHCP) antenna. As a result the minimum received power specified at a RHCP antenna for L1 C/A code is -159.6 dBw. In actual practice the power of the satellite signals are designed such that they will continue to meet power specifications at the satellite end-of-life. As a result newer satellites tend to output signals which may be up to 6 dB stronger than the -159.6 dBw specification. Variations in the satellite antenna gain, the receiver antenna gain, and atmospheric losses also impact the received signal power which enters the receiver [KAP96].

The development of the GPS interference signal characteristics was based on the work of Mr. A.J. Van Dierendonck [PAR96]. An interference signal spread by a PRN code produces noise that affects the effective signal-to-noise density S/N_o , in ratio-Hz,

$$\left(\frac{S}{N_o}\right)^{-1} = \left(\frac{S}{N_{OT}}\right)^{-1} + \left(\frac{S}{N_{OI}}\right)^{-1} \quad (2-2)$$

where N_{OT} is the spread thermal noise density and N_{OI} is the spread interference noise density. The convolution of the spectral density of the code and the interference spectral density is the density of the noise or interference at the output of the correlator.

$$N_{OI}(f') = \int_{-\infty}^{\infty} S_c(f) S_I(f' - f) df \quad (2-3)$$

where $S_c(f)$ is the spectral density of the reference PRN code and $S_I(f)$ is the density of the interference or noise. The reference C/A code has a discrete spectral density that may be described as follows:

$$S_c(f) = \sum_{j=-\infty}^{\infty} c_j \delta(f - 1000j) \quad (2-4)$$

where c_j are spectral line coefficients, $\delta(f)$ is the dirac delta function, and the c_j vary about the envelope

$$c_j = 1000 T_{c/a} \frac{\sin^2(1000\pi j T_{c/a})}{(1000\pi j T_{c/a})^2} \quad (2-5)$$

where $T_{c/a}$ is $[1/1.023 \times 10^6]$ s. The spectral density of the reference PRN code has the property that

$$\int_{-\infty}^{\infty} S_c(f) df = 1 \quad (2-6)$$

Continuous wave interference has the following spectral density:

$$S_i(f) = P_i \delta(f - f_i) \quad (2-7)$$

where f_i is the frequency of the interference and P_i is the total interference power. For C/A code the post correlation noise density can take on the value of one of the spectral lines times the interference power, if centered on the spectral line. The resulting spectral density is a spectral line because the spreading would repeat every C/A code period.

$$N_{oi}(f'_i) = P_i c_j \delta(f'_i - f_i) \quad (2-8)$$

Equation (2-8) is valid if the spectral density is computed over a relatively long period of time and assumes that no data is modulated on the processed signal's C/A code.

Also, for relatively wide-band interference signals, the equations are valid since the resulting spread interference becomes noise, with a code bandwidth that is statistically independent over time. Furthermore, CW interference spread with the C/A code is not statistically independent over time. Since the signal code is modulated with the 50 Hz

data, the resulting spectral density components of interference can be computed only with a minimum bandwidth of 50 Hz. As a result the spectral density components of the CW interference are not exactly a line but rather a spread spectrum with a minimum bandwidth equal to the post-correlation receiver-processing bandwidth. Even though CW interference may not coincide with a C/A code spectral line, the interference will pass through the correlation process but with a reduced effect. Because of this it is very challenging to predict the effects of CW interference on the C/A code and normally the worst case effects are used. These effects are based on equation (2-8) for the largest C/A code spectral lines that can be roughly 9 dB larger than that of the c_j envelope [PAR96].

2.6 RECEIVER TRACKING LOOPS

The acquisition and tracking of the GPS signal is a two-dimensional process. Each tracking channel must track both the PRN code and the carrier phase/frequency with a Doppler offset for each satellite. It does this by generating a replica code and carrier signal as shown in Figure 2.3.

The code tracking is typically done in a Delay Lock Loop (DLL). A replica of the PRN code is generated within the receiver, and then shifted until it correlates with the satellite PRN code. The carrier tracking loop may be of the form of a Phase Lock Loop (PLL), a Costas PLL, or a Frequency Lock Loop (FLL). Factors such as

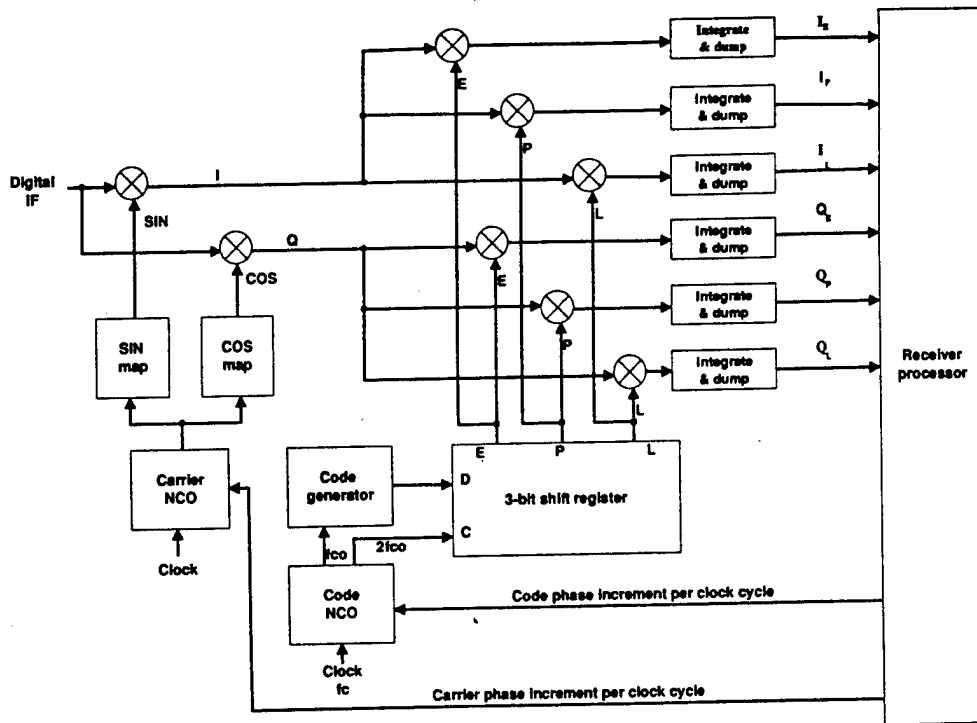


Figure 2.3 Generic Digital Receiver Tracking Channels [KAP96]

pre-detection integration time (PIT), carrier loop filter noise bandwidth, and dynamic stress affect the overall performance of the tracking loop. A Costas carrier tracking loop is commonly used in GPS receivers because Costas loops are insensitive to 180 degree phase reversals in the I and Q signals provided that the PIT of the I and Q signals do not straddle the data bit transitions [KAP96].

The acquisition threshold for a receiver is higher than the tracking threshold. Therefore, when RF interference reduces the C/N_0 of all GPS signals below the receiver's thresholds, the receiver will lose its ability to generate a valid navigation solution. In the case of CW interference it is feasible that the carrier tracking loop may actually lock on to the jamming signal as shown in Section 4.6. Navigation solution problems will occur due to incorrect signal phase and data bit synchronization.

2.7 DOPPLER SHIFT

The magnitude of Doppler shift varies depending on the relative velocity of the receiver and the satellites. A satellite at zenith is at the closest point of approach and has no radial velocity resulting in no Doppler shift. The maximum radial velocity of a satellite occurs at the horizon and is either positive or negative resulting in maximum Doppler shift of approximately ± 6 KHz. Frequency error and drift of satellite and user clocks also affects the Doppler shift measurement [PAR96].

The GPS receiver must account for the Doppler shift relative to the receiver's local oscillator. A numerically controlled oscillator (NCO) is used in a GPS receiver to

control the carrier tracking loop. The observed frequency shift of the received signal from the NCO is a measure of the Doppler shift [PAR96].

Different Doppler frequencies for each satellite provide an opportunity to target particular satellites for being jammed at the receiver. Because GPS orbits have repeating ground tracks, Doppler frequencies can be predicted for each satellite based on satellite ephemeris data and a given user location. An adjustment is required due to the approximate four minute difference in a solar day and sidereal day. These Doppler characteristics were used to investigate the feasibility of selectively jamming a specific satellite PRN signal, as highlighted in Section 4.6.

2.8 C/N₀ AND J/S CALCULATIONS

The Signal to Noise ratio or C/N is commonly used as a measure of a receiver's tracking threshold. Noise power is spread over a wide bandwidth while the GPS satellite signal of interest is spread over a narrow bandwidth. Filters in the receiver are used to narrow the signal bandwidth of interest in order to receive the minimum amount of noise and at the same time the maximum amount of signal. The term, C/N₀, is the carrier to noise power ratio in a 1 Hz bandwidth (dB-Hz). The derivations in this section are taken from Mr. Ward's work presented in [KAP96], [WAR95], and [WAR98].

The equation for un-jammed C/N_o at base-band is given by the equation:

$$\frac{C}{N_o} = S_r + G_a - 10 \log(kT_o) - N_f - L \text{ (dB-Hz)} \quad (2-9)$$

where:

S_r	=	received GPS signal power (dBw)
G_a	=	antenna gain toward the satellite (dBic)
$10\log(kT_o)$	=	thermal noise density (dBw-Hz) = -204 dBw-Hz
k	=	Boltzman's Constant (watts-seconds/K) = 1.38×10^{-23}
T_o	=	thermal noise reference temperature (K)
	=	290 K
N_f	=	noise figure of receiver including antenna and cable losses
(dB)		
L	=	implementation losses plus A/D converter losses (dB)
C	=	Total received Signal Power
N_o	=	Noise Power Density of the system

As an example, using received satellite signal power, $S_r = -159.6$ dBw, an antenna gain $G_a = 0$ dBic, a receiver noise figure, $N_f = 4$ dB, and implementation losses, $L = 2$ dB, result in a C/N_o of 38.4 dB-Hz [KAP96].

In the presence of RF interference, the unjammed C/N_o is reduced to an equivalent carrier to noise density ratio. Normally the lower case terms, c/n_o , are used when the expression is a dimensionless ratio, and upper case is used when it is expressed in dB-Hz. The equivalent (eqv) c/n_o provides the relationship between unjammed c/n_o and the jamming to signal ratio as follows:

$$\left[\frac{c}{n_o} \right]_{eqv} = \frac{1}{\left(\frac{1}{c/n_o} \right) + \frac{j/s}{Q \cdot f_c}} \quad \text{(power ratio)} \quad (2-10)$$

where:

- c/n_o = unjammed carrier to noise power in a 1 Hz bandwidth (ratio)
- j/s = jammer to signal power (ratio)
- f_c = GPS PRN code chipping rate (chips/sec) = 1.023×10^6 for C/A code
- Q = spread spectrum processing gain adjustment factor
- = 1.0 for narrowband jammer
- = 1.5 for spread spectrum (wideband jammer)
- = 2.0 for wideband (Gaussian) jammer

This equation may be written in terms of dB-Hz as follows:

$$\left[\frac{C}{N_o} \right]_{eqv} = -10 \log \left[10 \left\{ \left(\frac{c}{N_o} \right) / 10 + \frac{10 \left(\frac{j}{S} \right) / 10}{Q \cdot f_c} \right\} \right] \quad \text{(dB)} \quad (2-11)$$

where:

- C/N_o = unjammed carrier to noise power in a 1 Hz bandwidth (dB-Hz)
- = $10 \log(c/n_o)$
- J/S = jammer to signal power ratio (dB)
- = $10 \log(j/s)$

When expressed in terms of J/S , the equation becomes

$$\left[\frac{J}{S} \right] = 10 \log \left[Q \cdot f_c \left[\frac{1}{10^{\left(\frac{C}{N_o} \right)_{\text{eqv}} / 10}} - \frac{1}{10^{\left(\frac{C}{N_o} \right) / 10}} \right] \right] \quad (\text{dB}) \quad (2-12)$$

and substituting in values for $Q=1$ (for narrowband jamming), $f_c = 1.023 \times 10^6$ for C/A code, optimistic values for a tracking threshold $[C/N_o]_{\text{eqv}}$ of 28.0 dB-Hz and a typical C/N_o of 38.4 dB-Hz results in a J/S of 31.7 dB.

Navstar, the manufacturer of the XR5-M, provided basic technical details of the XR5-M receiver design which are included in Appendix D; however, typical ranges for C/N_o from the XR5-M operating manual were reported as between 33 and 50 dB-Hz.

Finally, the J/S jammer to signal power ratio in dB may be written as

$$\left[\frac{J}{S} \right] = J_r - S_r \quad (\text{dB}) \quad (2-13)$$

where

- J_r = received (incident) jammer power into the receiver (dBm)
- S_r = received (incident) signal power into the receiver (dBm) [WAR95].

2.9 PREVIOUS GPS MODELING AND SIMULATION AT AFIT

A brief synopsis is provided of previous AFIT thesis research into GPS receiver design and/or digital filter designs. The research by Captain Vasquez, Captain Falen, and Captain Harris provided beneficial background information.

Captain Juan Vasquez conducted research into failure detection and isolation techniques using an extended Kalman filter. Analysis was conducted using a Kalman filter development package known as the Multi-mode Simulation for Optimal Filter Evaluation (MSOFE). Captain Vasquez' results indicated that "failures within the GPS could be detected, isolated, and in some cases compensated through feedback" [VAS92].

Captain Gerald Falen conducted thesis research in 1994 into the "Analysis and Simulation of Rejection of Narrow-band GPS Jamming Using Digital Excision Temporal Filtering (DETF)." The results of this research indicated that a DETF could effectively reject all types of simulated jammers except for the wide-band noise jammer. The simulation results indicated that the DETF actually degraded the GPS system performance in the presence of a wide-band noise jammer [FAL94].

Captain George Harris conducted research into the performance of two types of tracking loops used in GPS receivers. The Delay Lock Loop (DLL) and the Modified Tanlock Loop were modeled both standalone, and combined. Individually the tracking loop results highlighted tracking lock across a wide range of loop gains and signal to noise ratios. When combined; however, the loops did not perform as well as theory predicted [HAR93].

2.10 CHAPTER SUMMARY

This chapter provided an overview of the signal characteristics of the Global Positioning System and the development of GPS jamming requirements. Further details regarding sources of RFI and means of mitigation of RFI are provided at Appendix G. Based on the GPS signal characteristics discussed in Chapter 2, jamming scenarios were developed in Chapter 3 and then applied to actual GPS signals.

III. EQUIPMENT CONFIGURATION AND TEST SET-UP

3.1 CHAPTER OVERVIEW

This chapter provides a description of the equipment test configuration used during the course of the thesis research. Further discussion of the equipment's technical characteristics, settings and software configuration are provided in Appendix D and E. The equipment used in the research included two commercial-off-the-shelf (COTS) Navstar XR5-M 12 channel GPS receivers, a Hewlett Packard (HP) signal generator, an HP spectrum analyzer, and an HP variable attenuator.

3.2 DIFFERENTIAL GPS (DGPS)

A C/A Code receiver is susceptible to several sources of position errors including Selective Availability (SA), ionospheric and tropospheric delays, space perturbations, receiver noise and multipath. The overall error is typically 100 meter 2DRMS. These error sources make it difficult to ascertain whether observed position errors are due to RF interference or due to other sources. By using DGPS, correlated errors are removed which allows relative positioning within a few meters.

The base station used a fixed XR5-M GPS receiver, operating at a known, surveyed location. It used the satellite signals to compute corrections which represented the signal errors introduced by ionospheric propagation, SA, etc. Because the base station antenna was at a known surveyed location, the total of the measured errors in each pseudorange were then sent via an RTCM link to the mobile receiver. The

antennas had a very short baseline (4.70 meters) resulting in highly correlated errors. The mobile receiver then determined position to DGPS accuracy. In the case of this research the two XR5-M RTCM data link ports were connected directly via a cable.

The XR5-M with firmware version 3.7 uses RTCM output messages for reported accuracy better than 3 meters circular error probable (CEP) [NAV96]. Real-time position with sub-meter accuracy using RTCM 20 & 21 message types would be feasible with a firmware/software upgrade to the latest version to the XR5-M although this was not considered necessary for this research. The upgrade would have provided the capability to obtain more accurate measurements and any individuals interested in conducting future research may wish to pursue the upgrade.

The base station antenna location was located within 8.20 meters of the "ALGN MARK" position based on the 1988 survey (Appendix A and B). The three 1988 surveyed locations on AFIT rooftop were "Doppler Station 32058," "ALGN MARK," and "GPS Antenna Mark (Bolt)." For the purpose of this research, the relative position between antenna was of greater interest and as such the position of the previously surveyed alignment mark "ALGN MARK" was used for the Base station coordinates. No corrections were applied to this error since the receivers were used in a relative differential GPS configuration. The distance between the base station antenna and the mobile antenna was measured as 4.70 meters. The actual position of the mobile antenna was corrected to the base station position in post processing. The remaining position error measured by the mobile receiver was a result of receiver noise, multipath and errors caused by RF interference to the mobile receiver.

An option of using a single GPS antenna with the two receivers was considered, but there were several unknowns, and thus this option was not selected. There was concern that impedance mismatch and damage to the antenna pre-amplifier could result. The two main benefits of this option are that the multipath error would be common to both receivers and thus could be eliminated easily, and no post processing correction would be required for distances between the base station antenna and the mobile antenna. Should the option of a single antenna with a pre-amplifier driven by two receivers prove feasible, it would be the recommended configuration for this sort of testing in the future. The use of an electrical component to block the DC power signal on one of the receiver cables to the antenna may prevent antenna pre-amplifier damage. This may allow a suitable configuration where only one of the receivers drives the antenna pre-amplifier.

3.3 RTCM MESSAGE FORMATS

The XR5-M receiver uses RTCM Type 1, 2, 3 and 9 messages in the differential corrections sent through the RTCM port. The RTCM Type 1 messages contain pseudorange and range-rate correction only, consequently the accuracy achievable is approximately 3 meters. Type 1 messages can accommodate up to 12 pseudorange corrections whereas Type 9 messages are similar in format but restricted to a maximum of three pseudorange corrections per message. RTCM Type 2 messages contain delta-pseudorange corrections, transmitted for a period of approximately 5 minutes following a satellite ephemeris upload. If selected these corrections enable more accurate

positions to be determined during the ephemeris transition. Finally, RTCM Type 3 messages contain the co-ordinates of the base station transmitted twice an hour at 15 and 45 minutes past the hour [NAV96].

3.4 EQUIPMENT CONFIGURATION

The main hardware components used during this research were two COTS Navstar XR5-M 12 Channel GPS Receivers used in conjunction with Navstar software version 3.7. The XR5-M has a volt rating of 11-32 volt DC, and is suitable for nominal 12, 24 , or 28 volt systems. The unit is also reverse voltage protected. The red and white leads were connected to the positive supply, the black lead to the negative supply, and the green lead to ground for screening [NAV96]. A screened data cable was grounded at the XR5-M connector end to minimize interference. Power connection wiring was as short as practicable, and not shared with heavy current and intermittent devices.

The face of the XR5-M receiver is shown in Figure 3.1 and highlights the receiver ports. The computer display unit (CDU) and RTCM Ports are bi-directional RS232D for control and data interchange. The RTCM port was used for the transfer of differential corrections. The RECORDER port is RS422A (compatible with the NMEA function) and normally operates as an output only. The recorder port may be used to log data on to a PC or other peripheral device; however, it was not used during the thesis research. Instead, data were recorded using the XR5-M CDU port connected to the PC COM1 port and using the XR5-M data monitor software program [NAV96].

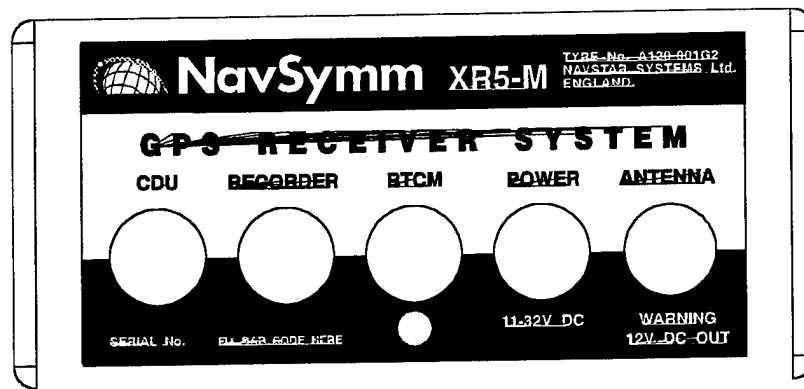


Figure 3.1 - XR5-M Receiver [NAV96]

Two Navstar GPS volute antennas with built in pre-amplifiers were located on the AFIT Building 640 rooftop. Each antenna was affixed to an individual bracket that was in turn anchored to a 1.25 inch diameter pipe using a U-bolt and then secured to existing AFIT rooftop structure. In order to reduce the effects of multipath, a choke ring antenna would have been preferred for the DGPS application.

A Hewlett Packard (HP) HP8643A 0.26-2060 MHz Signal Generator was used to generate CW and swept CW signals as specified for the Test 1 to 12 scenarios developed in Section 3.6. An HP Variable Attenuator Model Number 394A was used to vary the signal level output by the Signal Generator. An HP Spectrum Analyzer HP8563A was used to measure the jamming signal characteristics. Both the HP signal generator and spectrum analyzer were programmed to match the individual test scenario configurations to expedite the switching between settings within each test. This was especially beneficial during the swept CW tests.

Cable and connector losses were measured at the L1 frequency using the signal generator and spectrum analyzer. The losses were then applied to the actual jamming signals for each of the jamming scenarios presented in Section 3.6.

Both receivers were connected to 80486 PCs and communication was via the Navstar XR5-M software running under MSDOS. The PC (CDU) was used to control the receiver initialization, configuration and for capturing GPS data (the data was saved in an ASCII format).

The Data Monitor software, provided with the XR5-M, was used to generate a specific set of variables that could then be captured to a data file. The data files were then edited using a text editor to strip off the header and footer text from the files, leaving just the data. The Mathworks™ Software MATLAB® version 5.2 was used on a Macintosh™ PowerPC® and a 400 MHz Pentium® II PC platform for the loading and analysis of the data files. The data files varied in size between 3.3 and 17.4 Megabytes depending on the number of variables captured, the total sample time and the data sample rate. Figure 3.2 highlights the equipment as configured for Tests 1 to 12 in Section 3.6

3.5 MEASUREMENT OF GPS AND JAMMING SIGNALS

One of the challenges of determining J/S is the magnitude of signal levels involved. As has been discussed, several factors impact on actual measured received signal values. Variations in the output power by different satellites due to age, satellite antenna gain pattern, the receiver antenna gain pattern, and atmospheric losses all

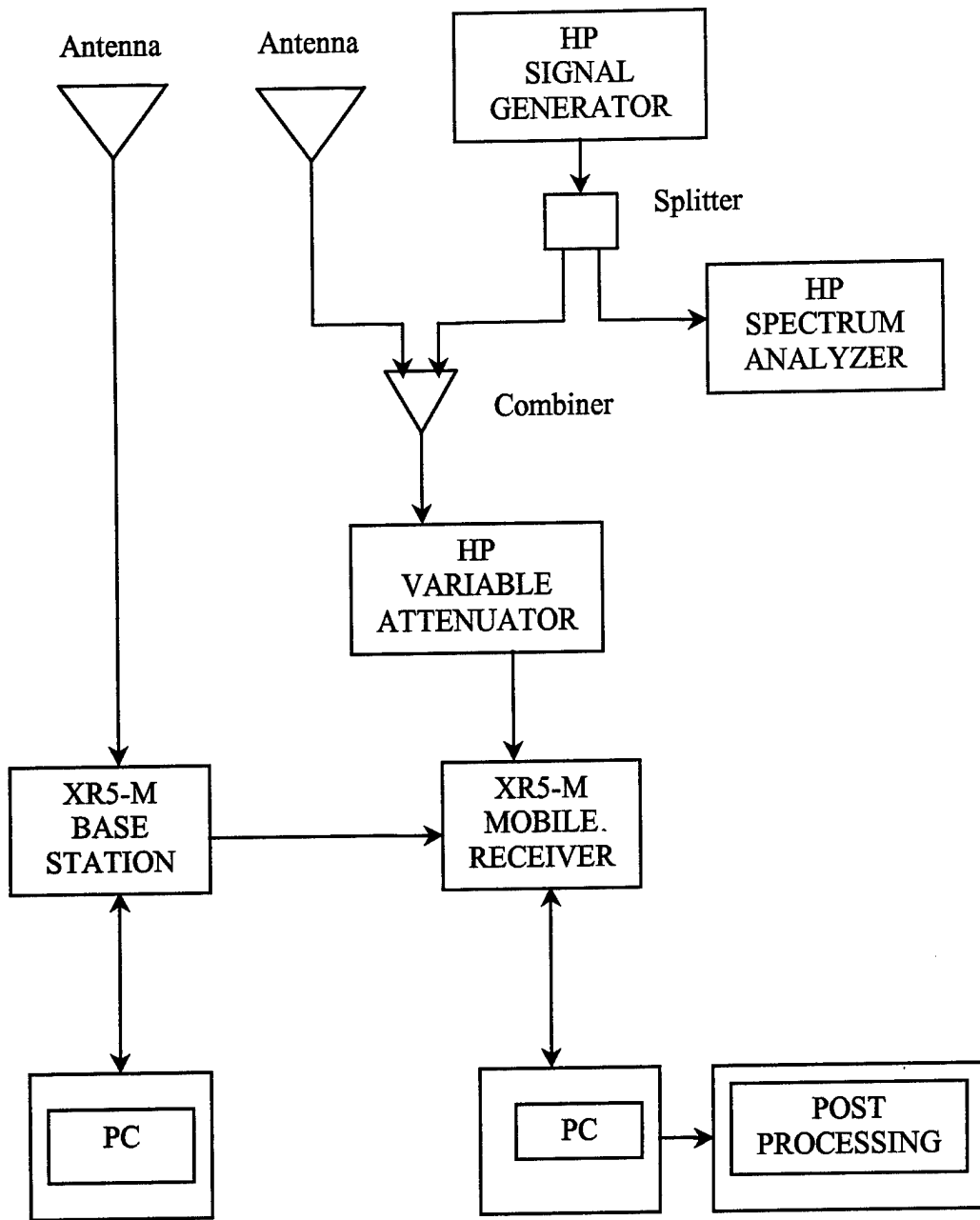


Figure 3.2 - Equipment Test Configuration

impact the actual received signal power. For this thesis research actual live GPS signals were used. If a GPS simulator was used, the signals must output correct signal levels by adjusting for system losses and gains.

If one simply connects a spectrum analyzer to measure the GPS signals, only noise will be observed since the strength of GPS signals at the analyzer are below the noise threshold. As a result there is no immediate means of measuring received satellite signal power. As an alternative, values for C/N_0 may be captured for all receiver tracking channels, (an XR5-M for this research). A general sense of the relative received signal levels may be observed between receiver channels.

For the purpose of this thesis the received signal power was considered to meet the GPS specifications of at least -129.6 dBm (-159.6 dBW) incident power received at the GPS antenna. The receiver antenna/pre-amplifier gain was taken from manufacturer specifications as 20 dB [NAV96]. Cable and connector losses were measured at L1 for both jamming and received signals.

The CW jamming signal was measured prior to entering a variable attenuator. This equipment setup was required because the CW jamming output of the variable attenuator was near the noise floor of the spectrum analyzer.

Jamming and the GPS signal measurement errors combine into an overall J/S amplitude error during testing. The focus of this thesis was on the ability to selectively jam satellite signals at the receiver, for the relative differences between low and high jamming levels, and the differences in position error for CW and swept CW jamming.

Based on the results of Equation 2-12, J/S ratios between 20.7 and 45.7 dB were investigated during preliminary testing to validate receiver thresholds.

3.6 JAMMING SCENARIOS

This section describes the twelve tests that were developed based on the GPS signal characteristics from Chapter 2. Elevation mask angle was set to five degrees for all tests with the exception of Test 8 (elevation mask angle of 25 degrees). Baseline performance of the XR5-M receiver with no jamming was investigated in Tests 1 and 2 as highlighted in Table 3.1. Each sample consisted of a subset of the variables outlined in Appendix C.

Test Number (Date)	Jamming Parameters
1 (20 Nov 98)	No Jamming Sample Rate:(one sample per 5 seconds) Test Duration: 1555Z-2002Z
2 (30 Nov 98)	No Jamming Sample Rate:(one sample per second) Test Duration: 1500Z-1730Z

Table 3.1 - No Jamming Tests

The two primary forms of jamming used were CW and swept CW. J/S levels were set between 20.7 and 40.7 dB and the center frequency was normally set near L1. Parameters for CW jamming included center frequency and jamming power level. The XR5-M receiver was subjected to CW jamming as outlined in Tests 3-8 as shown in Table 3.2.

Test Number (Date)	Jamming Parameters
3 (16 Nov 98)	Center Frequency (MHz):1575.420010 J/S (dB): 20.7 Sample Rate: One sample per 5 seconds Test Duration: 1603Z-2007Z
4 (27 Nov 98)	Center Frequency (MHz):1575.419305 J/S (dB): 35.7 Sample Rate: One sample per second Jam Target: PRN # 15, 29 Test Duration: 1554Z-1700Z
5 (2 Dec 98)	Center Frequency (MHz):1575.421960 J/S (dB): 35.7 Sample Rate: One sample per second Jam Target: PRN # 25, 29, 30 Test Duration: 1500Z-1730Z
6 (3 Dec 98)	Center Frequency (MHz):1575.482950 J/S (dB): 25.7 Sample Rate: One sample per second Jam Target: PRN # 29, 30 at lower level Test Duration: 1500Z-1730Z
7 (8 Dec 98)	Center Frequency (MHz):1575.420010 J/S (dB): 20.7, 25.7, 30.7, 35.7 Sample Rate: One sample per second Test Duration: 1500Z-1710Z
8 (11 Dec 98)	Center Frequency (MHz):1575.419930 J/S (dB): 20.7, 25.7, 30.7, 35.7 Elevation Mask Angle Raised to 25 Degrees Sample Rate: One sample per second Test Duration: 1510Z-1710Z

Table 3.2 - CW Jamming Tests

For swept CW jamming, the center frequency was centered on the sweep bandwidth over the sweep duration. The swept CW jamming parameters included center frequency and power level, sweep bandwidth and sweep duration. Dedicated swept CW jamming was conducted in Test 9, 10 and 11 as highlighted in Table 3.3.

Test Number (Date)	Jamming Parameters
9 (6 Dec 98)	Center Frequency (MHz):1575.419950 J/S (dB): 20.7, 25.7, 30.7, 35.7, 40.7 Sweep Bandwidth: 2 MHz, 200 kHz, 20 kHz Sweep Duration: 20 seconds Sample Rate: One sample per second Test Duration: 1500Z-1700Z
10 (7 Dec 98)	Center Frequency (MHz):1575.419950 J/S (dB): 20.7, 25.7, 30.7, 35.7, 40.7 Sweep Bandwidth: 20 kHz, 10 kHz Sweep Duration: 20 seconds Sample Rate: One sample per second Test Duration: 1500Z-1710Z
11 (10 Dec 98)	Center Frequency (MHz):1575.419950 J/S (dB): 20.7, 25.7, 30.7, 35.7 Sweep Bandwidth: 2 MHz, 200 kHz, 20 kHz Sweep Duration: 1 seconds Sample Rate: One sample per second Test Duration: 1500Z-1710Z

Table 3.3 Swept CW Jamming Tests

Finally Test 12 was dedicated to investigating position error as a result of CW jamming as shown in Table 3.4

Test Number (Date)	Jamming Parameters
12 (17 Dec 98)	Center Frequency (MHz): 1575.419935 J/S (dB): 35.7 Sample Rate: One sample per second Jamming Periods - 10 minutes No Jamming Periods - 5 minutes Test Duration: 1430Z-1705Z

Table 3.4 - CW Jamming Position Error Measurements

3.7 CHAPTER SUMMARY

This chapter provided an overview of the equipment configuration used for jamming GPS signals in this thesis research. Further details of the equipment are contained in Appendix D and Appendix E. The jamming scenarios in Table 3.1, 3.2, 3.3 and 3.4 were used for Tests 1 to 12. Results for Tests 1 to 12 are discussed in Chapter 4 and the associated plots are contained in Appendix I to Appendix T.

IV. RESULTS AND ANALYSIS

4.1 CHAPTER OVERVIEW

Although each GPS satellite transmits at the same L1 frequency, the relative motion between each satellite and the receiver causes the Doppler shifted frequency to be different for each satellite. In addition, each satellite transmits a different PRN code. These two characteristics make each GPS satellite signal received unique and it was these characteristics that were used to investigate the feasibility of selectively jamming a GPS satellite.

In order to develop an appreciation for the various effects of CW and swept CW jamming on the XR5-M receiver, preliminary testing was conducted 6-15 November 1998. This chapter presents the experimental results and an analysis of the results for the data gathered between 16 November and 17 December 1998 based on the twelve tests developed in Chapter 3. Figures for Tests 1 to Test 12 are provided in Appendix I to Appendix T respectively.

4.2 EQUIPMENT CONFIGURATION

The equipment was configured as shown in Chapter 3, Figure 3.2, using two Navstar XR5-M GPS receivers, a Hewlett Packard (HP) HP 8643A Signal Generator, an HP8563A Spectrum Analyzer, and an HP Variable Attenuator Model Number 394A. One of the XR5-M receivers was used as a base station and transmitted differential corrections directly to the second XR5-M receiver operating as a mobile receiver. The HP Signal Generator was used to generate CW and swept CW signals and the HP

Variable Attenuator was used to set various jamming levels. Further details of the XR5-M receivers are provided in Appendix D, and details of the HP equipment are provided in Appendix E.

4.3 JAM TO SIGNAL MEASUREMENTS

The specified L1 C/A signal level received from the satellites was -160 dBW. This value was adjusted according to Mr. P. Ward [KAP96] for the differences in antenna polarization to -159.6 dBW (-129.6 dBm). Using measured cable/connector losses between the antenna and the receiver of 16.3 dB, and a specified antenna gain of 20 dB resulted in an overall L1 C/A code signal level at the receiver of -125.9 dBm. Table 4.1 provides a summary of the actual J/S for the output of the signal generator, the given attenuator settings, and the total cable/connector losses measured at L1 between the signal generator and the receiver.

Signal Generator Output (dBm)	Cable/Connector Losses Measured between Signal Generator and Receiver (dB)	Attenuator Setting (dB)	Jamming Signal Level Measured at Receiver (dBm)	L1 C/A Signal Level at Receiver (dBm)	J/S (dB)
-10	10.2	120	-140.2	-125.9	-14.3
-10	10.2	85	-105.2	-125.9	20.7
-10	10.2	80	-100.2	-125.9	25.7
-10	10.2	75	-95.2	-125.9	30.7
-10	10.2	70	-90.2	-125.9	35.7
-10	10.2	65	-85.2	-125.9	40.7

Table 4.1 - J/S Calculations

4.4 TEST RESULTS OVERVIEW

Jamming and no jamming tests were conducted over the period 6 November to 17 December 1998. A sub-set of the overall results is provided in this thesis which highlights the observations over the testing period. Test dates for Test 1 to Test 12 were not sequential. For example Test 3 was conducted 16 November 1998 while Test 1 and Test 2 were conducted 20 and 30 November 1998 respectively. Test periods were generally scheduled to look at a common set of satellites from test to test. A summary of the test parameters is provided in Table 4.2.

The results of Test 1 to Test 12 are discussed below and are plotted in Appendix I to Appendix T. The first two pages of Appendix I to T indicate the GPS satellite constellation configuration at specific times. A sample plot is shown below in Figure 4.1.

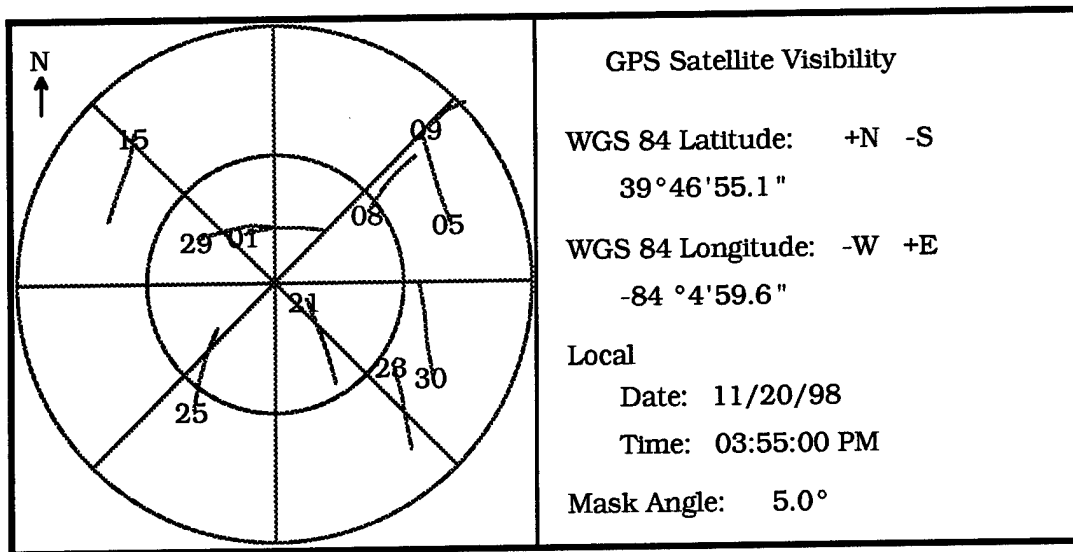


Figure 4.1 - Satellite Constellation 1555Z 20 Nov 98

TEST #	DATE	APDX.	CENTER FREQ OFFSET FROM L1 (APPROX) (HZ)	TOTAL FREQ SPAN (KHZ)	SWEEP RATE (SECS)	JAMMING LEVELS (J/S dB)	AIM
1	20/11/98	I	NO JAM	N/A	N/A	N/A	EST. BASELINE
2	30/11/98	J	NO JAM	N/A	N/A	N/A	EST. BASELINE
3	16/11/98	K	+10	N/A	N/A	JAM ON AT MINUTE 2 AT 20.7	INVESTIGATE LOW J/S
4	27/11/98	L	- 694	N/A	N/A	30.7 FOR FIRST SIX MINUTES, THEN NO JAM UNTIL MINUTE 24 WHEN LEVEL WAS SET AT 35.7	ATTEMPT TO JAM PRN 15 AND PRN 29
5	02/12/98	M	- 42	N/A	N/A	JAM ON AT MINUTE 80 AT 35.7	ATTEMPT TO JAM PRN 30 AND PRN 29
6	03/12/98	N	+ 62942	N/A	N/A	JAM ON AT MINUTE 75 AT 25.7	ATTEMPT TO JAM PRN 30 USING MAX SPECTRAL LINE AT RELATIVELY LOW J/S
7	08/12/98	O	+ 6	N/A	N/A	20.7, 25.7, 30.7, 35.7	INVESTIGATE IMPACT OF VARIOUS J/S LEVELS
8	11/12/98	P	- 70	N/A	N/A	20.7, 25.7, 30.7, 35.7	REDUCE IMPACT OF JAMMING BY RAISING ELEVATION MASK ANGLE TO 25 DEGREES
9	06/12/98	Q	- 60	2000, 200, 20	20	20.7, 25.7, 30.7, 35.7, 40.7	INVESTIGATE IMPACT OF SWEEP CW FOR GIVEN PARAMETERS
10	07/12/98	R	- 60	20, 10	20	20.7, 25.7, 30.7, 35.7	AS ABOVE
11	10/12/98	S	- 50	2000, 200, 20	1	20.7, 25.7, 30.7, 35.7, 40.7	AS ABOVE
12	17/12/98	T	- 63	N/A	N/A	35.7	INVESTIGATE POSITION ERRORS

Table 4.2 - Summary of Test Parameters

The vectors in the polar plots of Figure 4.1 indicate the direction of satellite travel as observed from the GPS antenna location on AFIT Building 640 rooftop. The PRN code for each satellite is labeled on the tail of each vector for current time with the head of the vector indicating future direction of travel. The times for the polar plots are for current local date and GPS (UTC) time (in 12 hour format). Current almanac data was downloaded to a GarminTM 12XL handheld GPS receiver and then downloaded to a MacintoshTM PowerPC[®]. The polar plots were generated using "MacGPS PRo[®] version 2.5.6" Software from James AssociatesTM. Polar plots were also generated from the XR5-M ephemeris data in MATLAB[®] and were compared with the GarminTM / MacintoshTM plots. The differences between ephemeris data and almanac data were not noticeable for the scale of plots used.

Unlike many twelve channel receivers in production today, the XR5-M receiver (using software version 3.7) selects only five satellites for the navigation solution. The five satellites chosen offers the lowest GDOP. The combination of five satellites used in the navigation solution is offered in the third figure for Appendix I to Appendix T, an example is shown in Figure 4.2.

The fourth figure in Appendix I to Appendix T indicates the PRN number assigned to each of the receiver tracking channels as shown in Figure 4.3. Typically Channel 11 was idle for most tests.

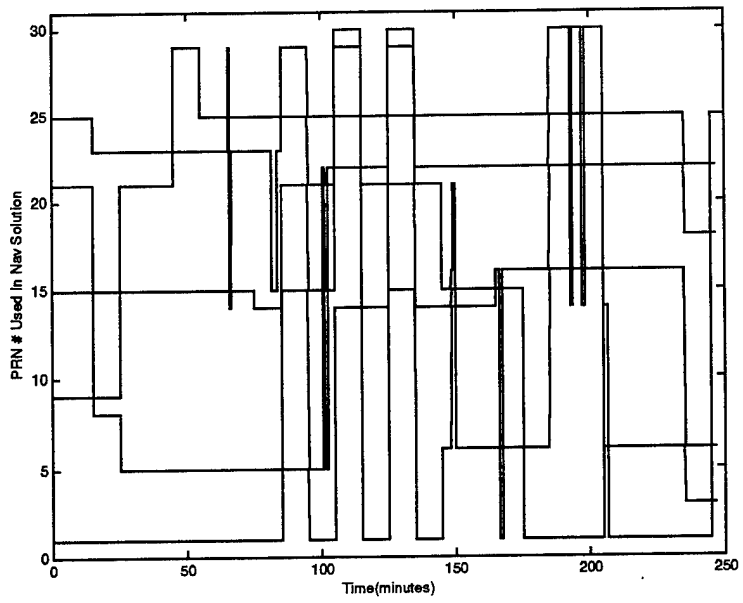


Figure 4.2 - PRN # Used in Navigation Solution versus Time

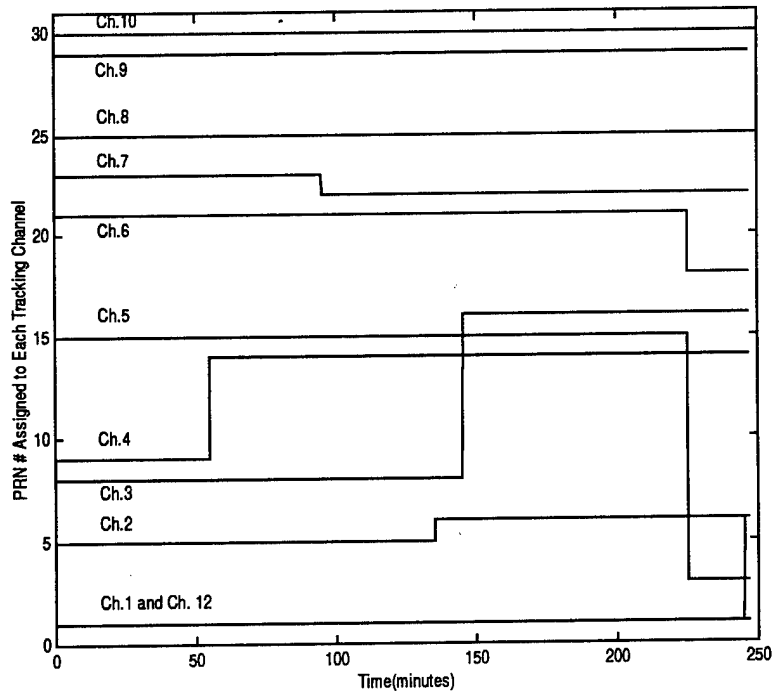


Figure 4.3 - PRN # Assigned to Each Tracking Channel versus Time

An example of the fifth figure in Appendix I to Appendix T, highlighting the GDOP values for the given navigation solution is shown in Figure 4.4. The reader should note that the scale for the vertical axis for each of the "double" GDOP plots was set to maximize the display, as a result, the scale for the two plots is normally different. During later jamming tests, the change in scale is of a larger magnitude than for Tests 1 and 2.

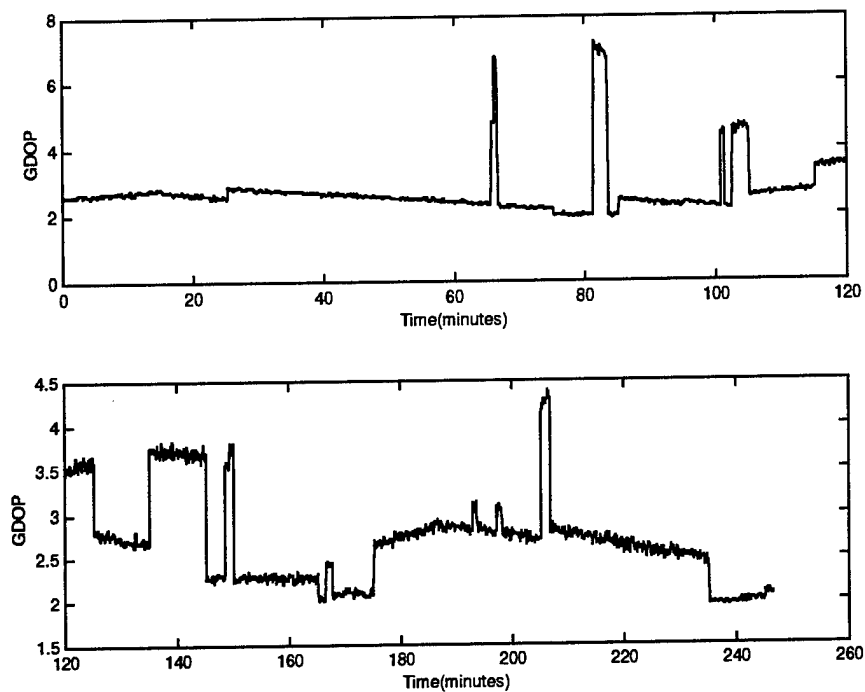


Figure 4.4 - GDOP versus Time

The remaining figures in Appendix I to T, show the Doppler frequency offset for each of the channels, the X,Y,Z and 3D ECEF position error of the mobile receiver antenna as compared to the base station, the receiver clock bias and drift, and finally the C/N_0 plots for each of the tracking channels. Examples of these plots are shown in Figures 4.5, 4.6, 4.7, and 4.8 respectively.

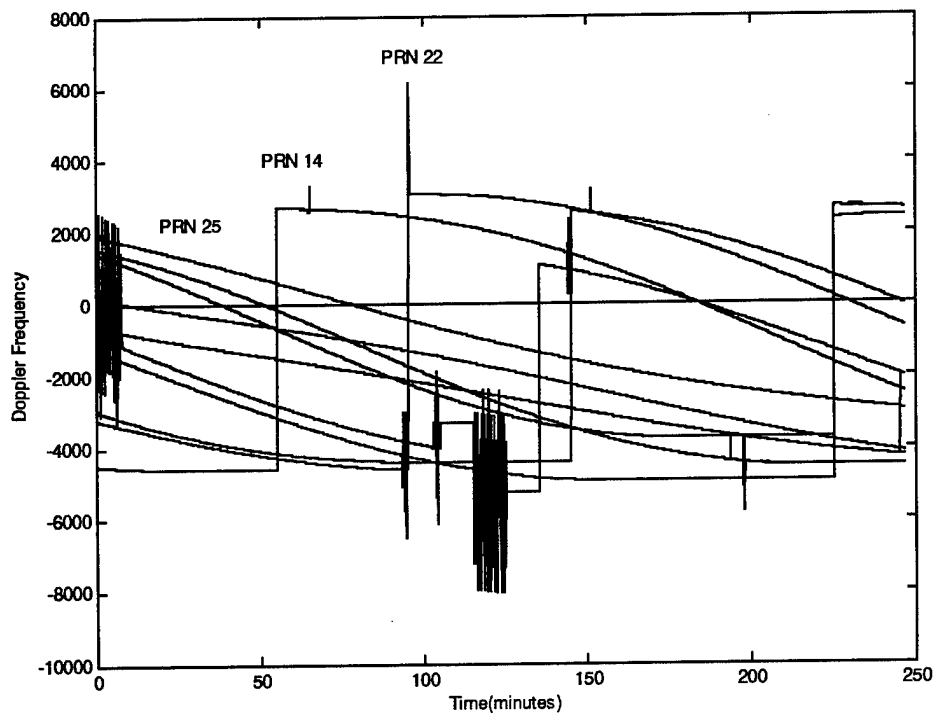


Figure 4.5 - Doppler frequency offset versus Time

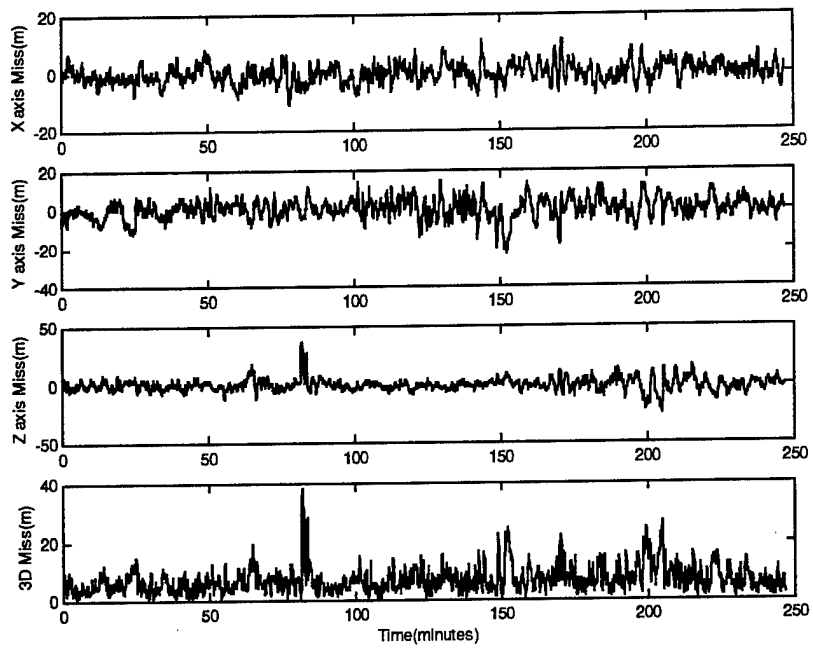


Figure 4.6 - X,Y, Z and 3D Error (meters) versus Time

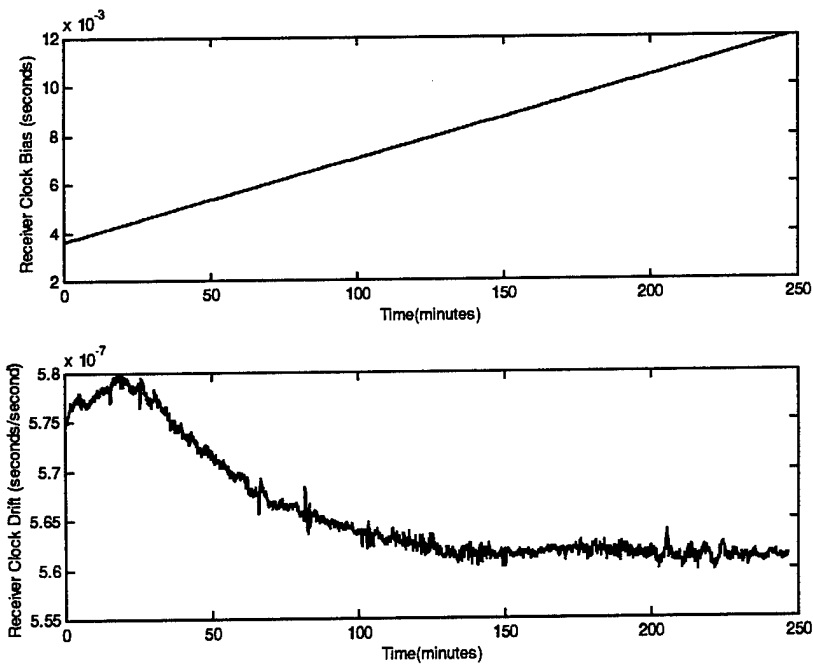


Figure 4.7 - XR5-M Receiver Clock Bias and Drift versus Time

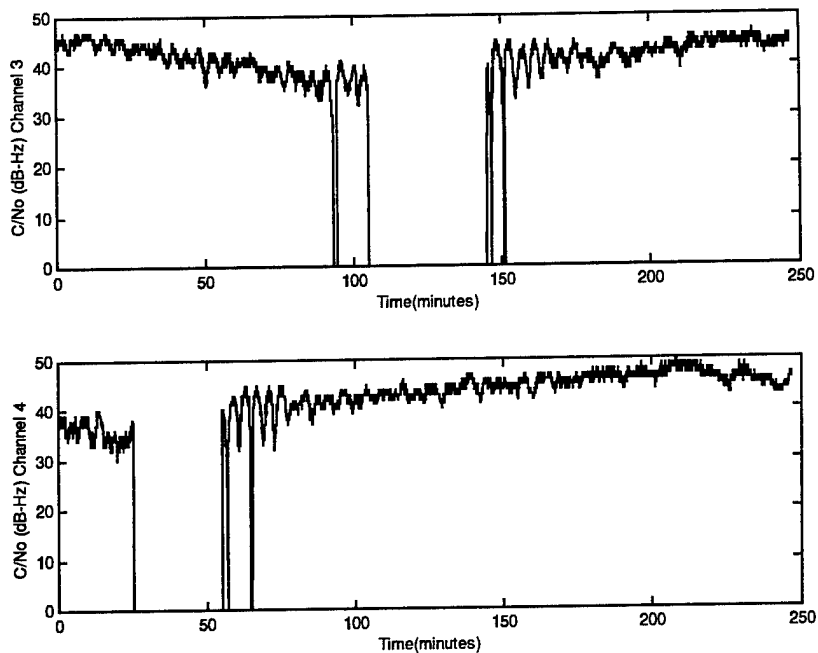


Figure 4.8 - C/N_0 versus Time

For the Doppler frequency offset plots, the associated PRN number for each of the tracking channels has been extracted from the combination of the channel number and the fourth figures of Appendix I to T in order to label each of the tracking channels with actual PRN numbers. It is still necessary to refer back to the third figure of Appendix I to T to match tracking channel number with PRN number for C/N_0 plots. For Test 9, 10, 11, and 12 an additional plot of J/S versus time is provided in Appendix Q, R, S and T respectively.

The elevation mask angle was set to 5 degrees for all tests with the exception of Test 8 where a receiver elevation mask angle of 25 degrees was used. The purpose of this change was to investigate the increase in elevation angle as a means to reduce the CW jamming effects on low elevation satellites.

4.5 NO JAMMING TEST RESULTS

This section discusses the results of Test 1 and Test 2 and the respective figures are contained in Appendix I and J.

4.5.1 TEST 1 RESULTS (FIGURES CONTAINED IN APPENDIX I)

Test 1 results for the data collected at a five second sample rate between 1555Z and 2001Z on 20 November 1998 under a no jamming scenario were analyzed and discussed below. A general sense of the receiver operation can be gathered from the polar plots of the satellite constellation in Figures I.1 and I.2 and the PRN number used in the navigation solution in Figure I.3. PRN 22 and 25 are shown at relatively high elevation angles and were used in conjunction with other satellites such as PRN 1, 5, 15 and 21. GDOP values from Figure I.5 typically ranged between 2 and 4 with a few exceptions, note the different scales on the vertical axis.

Although the XR5-M is a 12 channel receiver; software version 3.7 (which was used for the tests conducted in this research) used only five channels for calculating navigational information. It was also observed that channel 12 of the receiver tracks the same satellite as channel 1 of the receiver (provided channel 1 has lock on a valid satellite). Channel 12 is presumably used to measure receiver inter-channel biases by comparing the same satellite being tracked on channel 1 of the receiver. Generally, the receiver assigns satellites in view sequentially to each of the receiver tracking channels (Test 12 is a notable exception as discussed in Section 4.8.1). Each of the satellite PRNs assigned to each tracking channel is plotted in Figure I.4 in Appendix I. For

example, as shown in Figure I.4, the receiver tracking channels assigned at the beginning of the run are shown in Table 4.3.

Receiver Tracking Channel	PRN Number
1 and 12	1
2	5
3	8
4	9
5	15
6	21
7	23
8	25
9	29
10	30
11	0 (channel idle)

Table 4.3 - PRN Number Assigned to Receiver Tracking Channel

The assignment of a PRN to a particular tracking channel does not mean that the receiver is actually tracking that PRN. Plots of C/N_0 , as shown in Figures I.13 to I.18, provide a clear indication of the tracking status of each channel. A separate XR5-M variable indicating the status of each tracking channel was collected as a cross check to C/N_0 (Appendix C) but was considered redundant and therefore was not plotted. It is important to understand the relationship between the PRN number assigned to each tracking channel when analyzing the C/N_0 plots. Plots of C/N_0 are by channel number; as a result dramatic changes in C/N_0 values need to be cross-checked with the PRN assigned to each tracking channel. For example, the C/N_0 value may indicate going to a zero value upon losing lock and then it either may regain lock or it may switch to a new PRN. This is shown in Figure I.4 which indicates that channel 2 is tracking PRN 5 at

minute 103, from Figure I.13 channel 2 loses lock intermittently on PRN 5 and then shortly thereafter loses lock completely. At minute 140 channel 2 switches to tracking PRN 6 which is shown in Figures I.4 and I.13.

The three dimensional instantaneous position error was determined by taking the magnitude of the error vector in three dimensions. The mean of the overall error in each of the X, Y and Z directions was of both positive and negative values. For example assume two samples are taken; the first sample has an X, Y, Z measurement error of 2, -2, and 3 meters and the second sample has an error of -2, 2, and -3 respectively. Based on these two samples the mean in each of the X, Y, and Z direction would be zero. The magnitude of the error in three dimensions was calculated by taking the square root of the some of the squares for each sample. In this case, the magnitude of the error would be the root of 17, ie. 4.1 meters for both samples. The mean of these two 3D errors would be 4.1 meters. This technique was used because the focus of measurement error was on the instantaneous 3D error during jamming windows. Mean errors were taken as a check on the differentially corrected outputs during no jamming windows.

The overall position error in the ECEF coordinate system had a mean of -0.365 meters in the X direction, 0.0937 meters in the Y direction and -0.757 meters in the Z direction. The 3D position error was calculated to have a mean of 6.923 meters and a standard deviation of 4.293 meters. This position error was reasonable given the anticipated three meters CEP from the receiver specifications. There was likely a small error attributed to the base station location not being surveyed to the one meter

accuracy specified even though relative position error was the main error of interest [NAV96].

In DGPS mode multipath errors are normally the largest source of error and the use of two volute antenna would have contributed to this error. The volute antenna is designed for maritime use, ie. a rolling/pitching platform. As a result, the antenna maintains a reasonable gain at low elevation angles making it more susceptible to multipath effects. For the purpose of this thesis, the measured ECEF position error was acceptable. Further information on ECEF calculations is provided in Appendix B.

The magnitude of position error is also related to the correlation between increases in position error and increases in GDOP. For example, at minute 82 in Figure I.5 an increase in GDOP occurs, the associated increase in 3D position error above 30 meters is evident in Figure I.11.

Figures I.6 to I.9 provide insight into the actual Doppler frequency offset from the L1 carrier for each of the tracking channels. The L1 frequency is mixed in the receiver and reduced from RF to intermediate frequency (IF). During the first five minutes of Figure I.6 a wide swath is observed. A detailed look at the swath in Figure I.7 revealed that PRN 5 was in a search mode and finally gains lock at minute 8.

Since the two receivers were operated in a relative differential mode using separate antennas, the receivers were susceptible to different multipath effects. Excellent examples of multipath effects on PRN 14 were observed over the entire six week testing period for an azimuth of 318 degrees and an elevation angle of 8 degrees.

At minute 65 the spike in Doppler frequency on PRN 14 is evident in Figure I.8. Loss of lock by PRN 8 at minute 94 and PRN 5 at minute 103 is also shown in Figure I.8.

The C/N_0 for PRN 1, which was tracked by channel 1 and channel 12 (Figure I.4), appear nearly identical (Figure I.13 channel 1 and Figure I.18 channel 12). By expanding both of these plots to extreme levels, small differences could be seen between the two channels. For the purpose of this thesis, no further research was conducted comparing these two sets of values. It is believed that these differences are used to measure inter-channel biases. Channel 11 was idle throughout the period.

For most PRNs observed, once the receiver began tracking the satellite, the Doppler frequency offset was a positive value and reduced as the satellite approached the observer location. As the satellite moved away from the observer it demonstrated a negative Doppler frequency offset which increased in the negative direction. Note that although the Doppler frequency has a larger magnitude at lower elevation angles, the rate of change of Doppler frequency is smaller at lower elevation angles. Because of this, CW jamming signals will dwell for a longer period of time at the tracking loop bandwidths as the frequency of the tracking channels for low elevation satellites moves through the spectral 1000 Hz jamming frequencies. In Figure I.9 an interesting characteristic of PRN 3 was observed. The positive Doppler frequency offset actually increased in the positive direction for a period of approximately 30 minutes before the Doppler frequency offset finally started to decrease.

Note also that channel 7 was assigned to PRN 23 and switched to tracking PRN 22 at minute 95 as shown in Figures I.4, I.8, and I.16 (channel 7). At minute 225

channel 5 switches from PRN 15 to PRN 3 and channel 6 switches from PRN 21 to PRN 18 and as shown in Figures I.4, I.9, and I.15 (channel 5 and channel 6).

From Figures I.6, I.8 and I.9 it can be seen that there are occasions when two satellite PRN numbers have the same Doppler frequency offset. For example, PRN 15 and PRN 29 have a Doppler frequency offset of -617 Hz at minute 54 (1649Z). PRN 30 and PRN 29 have a Doppler frequency offset of -970 Hz at minute 76.5 (1711.5Z). PRN 1 and PRN 15 have a Doppler frequency offset of -2031 Hz at minute 90.1 (1725.1Z) and PRN 1 and PRN 30 have a Doppler frequency offset of -2394 Hz at minute 112.8 (1747.8Z). These basic characteristics of the intersection of Doppler frequencies were used to optimize the CW jamming tests.

Receiver clock bias was very linear, and the receiver clock drift rate settled out over the first 100 minutes Figure I.12. Earlier testing revealed an interesting event regarding receiver clock drift rate and the observed Doppler frequencies. For the time period used for testing, the Doppler frequency values typically ranged from +3.1 kHz to -4.9 kHz. This bias is discussed in greater detail in Section 4.9, Special Observations.

4.5.2 TEST 2 RESULTS (FIGURES CONTAINED IN APPENDIX J)

Test 2 results for the data collected at a one second sample rate between 1500Z and 1730Z on 30 November 1998 under a no jamming scenario were analyzed next. A general sense of the receiver operation can be gathered from the polar plots of the satellite constellation in Figures J.1 and J.2 and the PRN number used in the navigation solution in Figure J.3. PRN 1, 21, 25 and 29 are shown at relatively high elevation

angles and were used in conjunction with other satellites such as PRN 5 and 15. Figure J.4 relates the satellite PRNs being tracked by each receiver channel and Figures J.13 to J.18 indicate the C/N_0 for each of the tracking channels. GDOP values from Figure J.5 typically ranged between 2 and 4.

The Doppler frequency offsets are shown in Figures J.6 to J.9. In particular, the multipath effects on PRN 14 are evident in Figure J.7 at minute 80, 84 and 88. From Figure J.4 it was determined that PRN 14 was being tracked on channel 4. A review of Figure J.14 for channel 4 showed strong peaks and troughs in the C/N_0 during this time frame for PRN 14.

Further analysis of the C/N_0 plots for low elevation satellites revealed an interesting characteristic. As shown with PRN 14, both channel 3, PRN 8 in Figure J.14 (channel 3) and channel 8, PRN 23 in Figure J.16 (channel 8) exhibit periodic peaks and troughs in the C/N_0 . This periodic increase and decrease in C/N_0 is a characteristic of multipath effects observed at low satellite elevation angles. As the multipath signals change in phase with the relative change in path lengths due to the relative motion of the satellite and the user, the multipath error on the code chip increases and decreases as a function of the C/N_0 .

From Figure J.4 it was determined that PRN 5 was being tracked on channel 2, and PRN 8 was being tracked on channel 3. Figure J.8 is a detailed expansion of Figure J.6 highlighting PRN 8 and PRN 5 loss of lock at minute 98 and minute 100 respectively. Both PRN 8 and PRN 5 regained lock within a minute. As can be seen from the C/N_0 for these events in Figure J.14 channel 3, and Figure J.13 channel 2, the

loss of lock for one minute occurred. Channel 2 broke lock at 33 dB-Hz, and regained lock at 37 dB-Hz. Channel 3 broke lock at 32 dB-Hz and regained lock at 34 dB-Hz (a short spike to 55 dB-Hz appears). From Figures J.6 and J.13 (channel 2) it can be seen that PRN 5 broke and regained lock once more before finally losing lock completely. From Figures J.6 and J.14 (channel 3) it can be seen that PRN 8 finally broke lock at minute 120. The loss of lock for PRN 5 and PRN 8 can be related to low elevation angles from Figure J.2 for both satellites.

Although it is not immediately obvious from Figure J.6, PRN 15, which is tracked on channel 5, exhibited an interesting characteristic highlighted in Figure J.9. For an unknown reason the tracking channel broke lock for a five second period at minute 105, 109 and 112. The loss of lock occurred at Doppler offset frequencies of -2109 Hz, -2252 Hz and -2267 Hz for each of the five second periods respectively. The loss of lock was evident in the C/N_0 plot in Figure J.15 for channel 5. The loss of lock was not representative of multipath effects that exhibited large oscillations in Doppler offset frequency observed during the six weeks of testing. This event is discussed in further detail in Section 4.9, Special Observations.

The C/N_0 for PRN 1, which was tracked by channel 1 and channel 12 (Figure J.4), appeared nearly identical (Figure J.13 channel 1 and Figure J.18 channel 12). By expanding both of these plots to extreme levels, small differences were seen between the two channels. The receiver demonstrated similar clock bias and drift rates in Figure J.12 as for Test 1 on 20 Nov 98 (Figure I.12).

The overall position error in the ECEF coordinate system had a mean of -0.292 meters in the X direction, -0.428 meters in the Y direction and 0.987 meters in the Z direction. The 3D position error was calculated to have a mean of 5.848 meters and a standard deviation of 3.112 meters (see section 4.5.1 for the method used to calculate 3D position error). Other positional information included the example of position error and increases in GDOP.

At minute 82 and minute 96 in Figure J.5 an increase in GDOP occurred, the associated increase in position error above 20 meters is evident in Figure J.11. The changes in the combination of satellites used in the navigation solution, as shown in Figure J.3, resulted in GDOP changes, as shown in Figure J.5.

From Figure J.6 it can be seen that there are occasions when two satellite PRN numbers have the same Doppler frequency offset. For example, PRN 15 and PRN 29 have a Doppler frequency offset of -678 Hz at minute 70, (1610Z). PRN 30 and PRN 29 have a Doppler frequency offset of -1056 Hz at minute 93.2 (1633.2Z). PRN 1 and PRN 15 have a Doppler frequency offset of -1991 Hz at minute 103 (1643Z); and PRN 1 and PRN 30 have a Doppler frequency offset of -2370 Hz at minute 127 (1707Z).

The results from the first two weeks of pre-tests verified that the constellation generally repeated its ground track. However, each satellite appears earlier each day by approximately 3 minutes and 56 seconds (the difference in a mean solar day and a sidereal day). Results of Test 1 and Test 2 for four cases involving the intersection of Doppler frequency offsets are provided in Table 4.4 and highlight the advance of the ground tracks with respect to time. For example over a ten day period between 20 and

30 November 1998, the intersection of PRNs was expected to advance by 39.33 minutes (10 x 3 min 56 sec). The actual results for the intersection of the PRN 15 and 29, PRN 30 and 29, PRN 1 and 15, and PRN 1 and 30 are included in Table 4.4. By comparing Test 1 and Test 2 results with test data collected during the last three weeks of November 98 (not presented in thesis), the characteristics of the intersection of Doppler frequencies were determined and subsequently used to optimize the CW jamming tests.

For the case of a stationary/slow velocity receiver, ie. people walking/running, ships, or hovering helicopters, the additional Doppler shift due to receiver motion would be relatively small (5.255 Hz at L1 for every meter/second of range rate). With the knowledge of Doppler shift from each satellite and velocity of a target vehicle, it is feasible that a "smart stationary CW jammer" could be optimized to jam specific frequencies and hence specific channels in a GPS receiver.

	PRN 15 and 29		PRN 30 and 29		PRN 1 and 15		PRN 1 and 30	
20 Nov 98	-617 Hz	1649Z	-970 Hz	1711.52Z	-2031 Hz	1725.12Z	-2394 Hz	1747.81Z
30 Nov 98	-678 Hz	1609.59Z	-1056 Hz	1633.18Z	-1991 Hz	1643Z	-2370 Hz	1706.59Z
Delta	61 Hz	39.4 min	86 Hz	37.94 min	40 Hz	42.12 min	24 Hz	41.22 min

Table 4.4 - PRN Doppler Frequency Offset Intercepts

The advancement of ground track with respect to time can also be seen by comparing the satellite constellation for the same time of day between 1500Z 30 November 1998 in Figure J.1 and 1500Z 10 December 1998 in Figure S.1.

4.6 CW JAMMING TEST RESULTS

This section discusses the results of CW jamming conducted in Tests 3-8 and the respective figures are contained in Appendices K to P.

4.6.1 TEST 3 RESULTS (FIGURES CONTAINED IN APPENDIX K)

Data collected at a rate of one sample per five seconds for Test 3 between 1603Z and 2007Z on 16 November 1998 were analyzed. The test included no jamming for the first 2 minutes followed by a setting of 85 dB on the attenuator resulting in a J/S of 20.7 dB for the duration of the test.

An overview of the satellite constellation status is provided in Figures K.1 and K.2 and the satellite PRN numbers used in the navigation solution in Figure K.3. Figure K.4 relates the satellite PRNs being tracked by each receiver channel and Figures K.13 to K.18 indicates the C/N_0 for each of the tracking channels. GDOP values from Figure K.5 typically ranged between 2 and 5 over the first 160 minutes. At minute 169 and minute 187 GDOP was reported as 2000, indicative of the receiver having ceased generating a navigation solution.

Perhaps the most interesting aspect of the Test 3 results are that the receiver tracking channels actually lock on to the CW jamming signal and track the jamming signal rather than the actual GPS signal. The jamming was constant throughout the period and the receiver's ability to calculate a correct position actually degraded over time as different tracking channels locked on to the CW signal at different times (see position errors in Figure K.10). The lock of a tracking channel on to the CW signal was

characterized for periods of a fairly constant C/N_0 value commencing at minute 67 in Figure K.14 channel 4 (PRN 14) and commencing at minute 73 in Figure K.13 channel 2 (PRN 5). The jamming signal was set at L1. The spreading of the jamming signal by the multiplication of the jamming signal with the C/A spreading code in the receiver demonstrated the 1000 Hz spectral characteristics of the CW signal after reception by the receiver. Jamming lines occurred at 3008 Hz, 1011 Hz, -2992 Hz, -3989 Hz as shown in Figure K.6. Slight differences in the magnitude of the 1000 Hz spaced lines over time resulted from either a very slow drift in the signal generator or receiver clock drift rate over the jamming period.

In particular PRN 14 on channel 4 (Figure K.4) immediately locked on to the jamming signal at minute 67 when tracking channel 4 switched from PRN 9 to PRN 14 (Figure K.7). Figure K.14 channel 4 highlights the loss of PRN 9 at minute 27 and the lock of PRN 14 onto the actual CW signal at minute 67 at 3008 Hz. The C/N_0 for PRN 14 was approximately 35 dB-Hz (Figure K.14) while it was tracking the jamming signal up to the minute 120 point where channel 4 regained lock on the actual satellite signal PRN 14 (Figure K.8). (Notice the steady Doppler frequency offset during periods of a channel locked on to the CW signal in Figure K.7).

PRN 5 on channel 2 (Figures K.4 and K.7) locked on to the jamming signal at minute 73 at -2992 Hz; at minute 108 the tracking channel switched to PRN 22 but immediately locked on to the CW signal at 3011 Hz (Figure K.8) and continued to maintain lock on the CW signal until minute 130 when the tracking channel finally gained lock on PRN 22. The lock of channel 2 on to the CW signal is evident in the

C/N₀ plot in Figure K.13 for channel 2. The spike at minute 108 in the C/N₀ plot occurred at the transition of locking on to the CW signal for the two frequencies.

PRN 8 on channel 3 (Figure K.4) locked on to the jamming signal at minute 92 at -3989 Hz (Figure K.7) and at minute 137 the tracking channel switched to PRN 6 but immediately locked on to the CW signal at 1011 Hz (Figure K.8). The tracking channel locked on to PRN 6 at minute 140 and maintained lock until minute 151 when the channel locked on to the CW signal again. The lock of channel 3 on to the CW signal is evident in the C/N₀ plot in Figure K.14 for channel 3.

PRN 15 on channel 5 (Figure K.4) locked on to the jamming signal for a ten minute period starting at minute 160 at -3988 Hz (Figure K.8). The lock of channel 5 on to the CW signal is evident in the C/N₀ plot in Figure K.15 for channel 5 between minutes 160 and 170.

Quite interesting is the fact that while PRN 5 is locked on to the CW signal the receiver continues to include PRN 5 in the navigation solution for up to ten minutes. After reviewing several data runs over the first few weeks of testing it became clear that the receiver uses the best GDOP solution of satellites for which the receiver has carrier lock in order to determine which satellites to use in the navigation solution. This is an extremely dangerous navigation solution criterion if the receiver is used in a CW jamming environment. During this research, various reference material alluded to the fact that CW interference normally only impacts a single channel in a receiver due to the different Doppler frequencies for each channel. While this is true at low J/S values, the XR5-M receiver demonstrates a dangerous weakness in receiver design if a single

bad channel is allowed into the navigation solution. Clearly there is a need to be aware of the impact of CW interference on position error when designing GPS receivers.

Techniques to reduce RF interference are discussed further in Appendix G.

The best GDOP solution can occur with a combination of SVs including the one with carrier lock on CW and therefore the receiver includes the bad satellite as one of the five SVs used in navigation solution. Because of the lack of code and no data modulation, bit synchronization is clearly a problem; errors grow from the typical un-jammed seven meter error (observed in Test 1 and 2) to over 12 kilometers. The receiver is "intelligent" enough to recognize a problem based on valid fix criteria; however, position errors grow to very large values before the receiver finally flags the fixes as no longer valid. Test 12, Section 4.8.1, was designed specifically to investigate in detail the magnitude of position error when the receiver flags the fix as no longer valid.

At minute 187 position error had grown to over 100 km (Figure K.10) and the receiver "finally threw in the towel" and reset (Figures K.4 and K.12). Keep in mind that the receiver had flagged the position as invalid at a smaller position error value. From Figure K.6 and an expansion of the time frame in Figure K.9, the Doppler frequency offsets are dominated by the jamming signal. The C/N_0 plots of Figures K.13 to K.18 exhibit rapid switching between the actual satellite signals and the jamming signal as the receiver is reassigning different PRNs to each of the tracking channels. The receiver regains a valid fix for the last 30 minutes of the run using PRNs 1, 6, 14, 25 and 29. A further look at the Doppler frequency offset plot of Figure K.6 indicates

that these five satellites are the only satellites that have not locked on to jamming signals. In a sense the receiver was "hanging on by a shoestring."

At a relatively low J/S of 20.7 dB the satellites with low C/N₀, ie. near the horizon, were most likely to be jammed. This was demonstrated when PRN 14, 8, 5, and 22 locked on to the CW jamming signal (Figures K.1, K.2 and K.6). The receiver's ability to determine position degraded significantly whenever at least one of the PRNs locked on to the CW jamming and was included in the final navigation solution. This test verified the inherent problems of the XR5-M C/A code receiver even at low interference levels. Furthermore, it highlighted that a simple CW jamming signal could spoof this receiver to over 12 kilometers position error. Further analysis of this spoofing impact is highlighted in Test 12 (see section 4.8.1). Based on the results of this thesis, testing of other C/A code GPS receivers in the presence of CW jamming is highly recommended.

4.6.2 TEST 4 RESULTS (FIGURES CONTAINED IN APPENDIX L)

Data collected at a rate of one sample per second for Test 4 between 1554Z and 1700Z on 27 November 1998 were analyzed. The test included a quick look at jamming for the first 6 minutes with an attenuator setting of 75 dB followed by no jamming for 18 minutes. Jamming was set to 70 dB on the attenuator resulting in a J/S of 35.7 dB centered at -694 Hz offset from L1 at 1618Z for the duration of the test. The primary aim of this test was to investigate the feasibility of simultaneously jamming two PRNs, specifically PRN 15 and PRN 29. Jamming was selected on at minute 24

just prior to the calculated intercept frequency and time. The main difference between Test 3 and Test 4 was the increase in J/S and the change in sample rate to once per second.

An overview of the satellite constellation status is provided in Figures L.1 and L.2 and the satellite PRN numbers used in the navigation solution in Figure L.3. Figure L.4 relates the satellite PRNs being tracked by each receiver channel and Figures L.13 to L.18 indicate the C/N_0 for each of the tracking channels. Channel 11 was set to PRN 21 but remained idle throughout the test (PRN 21 was actually tracked on channel 6). GDOP values from Figure L.5 typically ranged between 2 and 4 over the first 35 minutes. At minute 37 GDOP was reported as 2000, indicative of the receiver having ceased generating a navigation solution.

The first 6 minutes of jamming were used to investigate the receiver when subjected to jamming shortly after gaining 3D lock, after initial power up of the system. Both PRN 8 and PRN 5 locked on to the jamming during the initial six minutes. From Figure L.3 it can be seen that PRN 5 was not used in the navigation solution but PRN 8 was used resulting in the increase in position error as just evident in Figure L.10 during the first few minutes of the test. The wave in Doppler frequency offset (Figure L.6 and Figure L.7) is believed to be a result of the receiver determining receiver clock drift rate from the navigation solution which can be seen in the clock drift rate over the first few minutes of the receiver operation, see Figure L.12. This wave effect is discussed in more detail in Section 4.9.2.

The test successfully demonstrated that an individual PRN could be intentionally jammed at the receiver. PRN 15 and PRN 5 locked on to the CW within 30 seconds of the commencement of jamming at minute 24 (Figure L.8) at Doppler frequencies of -694 Hz and -2694 Hz respectively. From Figure L.3 it can be seen that PRN 5 and 15 both momentarily were removed from the navigation solution as they succumbed to the jamming and C/N_0 went to zero very briefly (Figure L.15 channel 5, PRN 15, and Figure L.13 channel 2, PRN 5). Once locked on to the CW, PRN 5 and 15 were both being used in the navigation solution. The resulting position error can be seen in Figure L.11. Position error began to increase at minute 24.5. PRN 8 and 23 locked on to the CW approximately 2 minutes later (Figure L.8) at -4694 Hz. Clearly, the rate of change in position error (Figure L.11) increased at minute 26.5 as PRN 23 was used in the navigation solution. PRN 8 was added to the navigation solution at minute 32. By minute 32, four of the five PRNs used in the navigation solution were locked on to the CW signal and PRN 1 was the only satellite used in the navigation solution with valid data. From Figure L.10 position error was a maximum at 38 kilometers when the receiver ceased to output a navigation solution.

PRN 29 was at a higher elevation angle and less susceptible to jamming at initialization; however, at minute 37 the receiver had ceased outputting a navigation solution and PRN 21, 25, 29, 30 had all succumbed to the CW jamming (Figure L.9). At minute 37, PRN 25 locked on to 305 Hz, PRN 29 and 30 locked on to -695 Hz, and PRN 21 locked on to -3695 Hz. Additionally, PRN 5 jumped from being jammed at

-2695 Hz to -3695 Hz. Although a bit of a mute point by this time in the receiver, PRN 14 locked on to 2306 Hz at minute 39. At minute 57 the receiver regained a "shoestring fix" using PRN 1, 15, 29 and 30. From Figure L.9 and the C/N_0 plots it can be seen that these were the only satellites not locked onto the CW jamming signal.

One of the interesting aspects observed was the two minute periodic spikes in the Doppler frequency in Figure L.6 and expanded in Figure L.9. These spikes were also clearly evident in the C/N_0 plots of Figures L.13 to L.17 and Doppler offset frequency Figures L.6 and L.9 after minute 36. The spiking in the C/N_0 was attributed to a two minute time-out that caused each of the tracking channels to reset when the channels were unable to synchronize to the data frame within that period [BUT99].

4.6.3 TEST 5 RESULTS (FIGURES CONTAINED IN APPENDIX M)

Data collected at a rate of one sample per second for Test 5 between 1500Z and 1730Z on 2 December 1998 were analyzed. Test 5 was a repeat of Test 4 except that the jamming center frequency was offset by +1958 Hz from L1. Jamming was set to 70 dB on the attenuator resulting in a J/S of 35.7 dB. The intent of commencing jamming at minute 80 was to jam two PRNs simultaneously by targeting the intersection of the Doppler frequency for PRN 30 and PRN 29 at 1620Z.

An overview of the satellite constellation status is provided in Figures M.1 and M.2 and the satellite PRN numbers used in the navigation solution in Figure M.3. Figure M.4 relates the satellite PRNs being tracked by each receiver channel and Figures M.13 to M.18 indicate the C/N_0 for each of the tracking channels. Channel 11

was idle throughout the test. As shown in Figure M.5, GDOP values typically ranged between 2 and 4 over the first 99 minutes. However, at minute 99 GDOP was reported as fixed at 2000, indicative of the receiver having ceased generating a navigation solution for the remainder of the test (Figures M.3 and M.6). Multipath effects on PRN 14 on channel 4 were again observed at minute 72 (Figure M.7) with the characteristic peaks and troughs in the C/N_0 in Figure M.14 channel 4.

The Doppler frequency offset (Figure M.8) highlights the effect of jamming at minute 80. The actual CW jamming frequency was 1958 Hz above L1. PRN 25 was jammed and was followed by PRN 30 being jammed within two minutes. PRN 14, 5, 8 and 23 were all jammed; however, PRN 29 was not jammed. These results highlight that it is feasible to jam a particular satellite. The higher jamming levels required to jam higher elevation satellites cause a type of collateral damage in that PRNs closer to the horizon were more susceptible to jamming and tended to lock on to the CW signal as well.

From Figures M.8 and M.9 it can be seen that the frequencies at which the various PRNs were jammed were once again spaced by the 1000 Hz spreading of the CW jamming signal by the C/A code. One exception occurred in Figure M.9, where the tracking channel actually locked on to a signal that was exactly 500 Hz between the jamming lines of -1040 Hz and -2040 Hz at -1540 Hz. This event is the subject of further study.

The position error for the period of 80 to 100 minutes is shown in Figure M.11. At minute 99, all channels of the receiver were locked on to the CW signal except for

PRN 21 on channel 7 which maintained intermittent lock (Figures M.6 and M.16 channel 7). The two minute periodic spikes in the Doppler frequency previously observed in Test 4 were observed again in Figure M.9. These spikes are also evident in the C/N_0 plots of Figures M.13 to M.17.

The jamming in Test 4 was centered at -694 Hz from L1 while during Test 5 the jamming was offset from L1 by +1958 Hz. Based on the results of Test 4 and Test 5 it would appear that the +1958 Hz offset from L1 in Test 5 was slightly more effective in that 6 satellites were simultaneously jammed. In Test 4, four satellites were jammed shortly after jamming was initiated. In both Test 4 and Test 5, position errors exceeded 10 km within 5 minutes after jamming commenced.

4.6.4 TEST 6 RESULTS (FIGURES CONTAINED IN APPENDIX N)

Data collected at a rate of one sample per second for Test 6 between 1500Z and 1730Z on 3 December 1998 were analyzed. Test 6 differed from Test 4 and Test 5 by both a change in center frequency and jamming power level. The receivers were allowed to operate for the first 75 minutes with no jamming. During Test 6 the jamming center frequency was offset by +63 kHz from L1 and the jamming level was set at 80 dB on the attenuator resulting in a J/S of 25.7 dB at minute 75, the jamming was on for the remainder of the test. From Table 6.4 of [KAP96], PRN 30 is theoretically more susceptible to jamming than the other satellites at 63 kHz offset from L1. The intent of Test 6 was to investigate selectively jamming an individual satellite

signal using the characteristic strongest spectral line for a specific PRN C/A code at a moderately low J/S.

An overview of the satellite constellation status is provided in Figures N.1 and N.2 and the satellite PRN numbers used in the navigation solution in Figure N.3. Figure N.4 relates the satellite PRNs tracked by each receiver channel and Figures N.13 to N.18 indicates the C/N_0 for each of the tracking channels. Channel 11 was idle throughout the test. GDOP values typically ranged between 2 and 4 over the first 115 minutes. At minute 120 GDOP was reported as 2000, as shown in Figure N.5; however, the receiver had flagged position invalid as of minute 89.7 at a position error of 5.5 km. The receiver regained lock at minute 142 and retained lock for the remaining eight minutes of the test but was somewhat marginal given that only six tracking channels were not being jammed (Figures N.3, N.6 and N.9).

It can be seen that PRN 5 on channel 2 (Figure N.4) was the cause of the wide dark vertical swath in the Doppler frequency offset in Figure N.6 and expanded in Figure N.7. Multipath effects on PRN 14 were again observed in Figure N.6 and the corresponding C/N_0 plot of channel 4 in Figure N.14 highlights the oscillation in the C/N_0 . The appearance of multipath on PRN 14 at minute 76 in Figure N.8 may have been partially enhanced by the commencement of jamming at minute 75.

As shown in Figure N.8, within two minutes of the commencement of jamming, PRN 30 locked on to the jamming at -1058 Hz and PRN 8 locked on to the jamming at -4058 Hz. Also, PRN 5 locked on to the jamming signal at minute 88. PRN 30 was tracked on channel 10 and the jamming effects can be seen in the C/N_0 plot of Figure

N.17. PRN 8 was tracked on channel 3, and the jamming effects can be seen in the C/N_0 plot of Figure N.14 for channel 3. PRN 5 was tracked on channel 2 and the corresponding effects can be seen in the C/N_0 plot of Figure N.13 for channel 2.

Although PRN 8 and PRN 30 were jammed at minute 77, the two satellites were not being used in the navigation solution (Figure N.3). From Figure N.3 PRN 5 was used in the navigation solution during the timeframe between minute 75 (commencement of jamming) and minute 100. The locking of PRN 5 on to the jamming signal at minute 88 corresponds with the beginning of an increase in the position error in Figures N.10 and N.11. Interestingly, at minute 100, PRN 5 was removed from the navigation solution and replaced by PRN 8 (which was also jammed). Position error continued to increase as seen in Figure N.10 at minute 100 as PRN 8 was added to the solution. If the reader looks closely at the period from minute 100 to minute 115 it can be seen that PRN 8 switches to PRN 14 with the combination of other satellites (PRN 1, 15, 21, and 25) which results in a valid fix. Note however there is an increase in GDOP at minute 106 as a result of this new assignment. The inherent weakness of the XR5-M receiver is highlighted when the receiver opts to switch back to using PRN 8 in place of PRN 14 because of improved GDOP. Unfortunately position error begins to rapidly grow again. The receiver again switches to PRN 14 at minute 111 and obtains a valid fix but the GDOP once again increases. During the next combination the receiver selects PRN 14, 21, 25, 29 and 30. Unfortunately, again for the XR5-M receiver, PRN 30 is jammed (Figure N.6) and the position error continues to grow rapidly. Keep in mind throughout this increase in position error only one of the

five satellites in the navigation solution was locked on to the CW jammer. Furthermore it only took 3 of the receiver channels to be jammed to drive the receiver into a rapidly degraded state.

From the Doppler frequency offset plot of Figure N.9 and the various C/N_0 plots (Figures N.13 to N.17) the receiver tracking channels were more severely impacted by the jamming signal. The rapid spiking in C/N_0 plots associated with the vertical spikes in the Doppler frequencies indicates that the receiver was more vulnerable to interference than during the earlier stages of jamming even though there was no change in jamming levels.

It must be reiterated that the XR5-M receiver actually flagged the position error as no longer valid once the position error was 5.5 km at second 5384 into the run (minute 89 and 44 seconds). The insight into the XR5-M receiver calculations highlights the impact of a single jammed channel being used in the navigation solution and how the position error continued to grow over the period.

Test 6 results demonstrated the jamming of a selected PRN using the technique of selecting a center frequency at the maximum magnitude spectral line for a given PRN code. It was also noted in Table 6.4 [KAP96] that PRN 8 has a maximum magnitude at a spectral line of 66 kHz. This probably attributed to the jamming of PRN 8 given the 3 kHz spacing between PRN 8 and PRN 30 at the instance that both PRNs locked on to the CW, keeping in mind that the spectral lines would be mirrored through L1.

4.6.5 TEST 7 RESULTS (FIGURES CONTAINED IN APPENDIX O)

Data collected at a rate of one sample per second for Test 7 between 1500Z and 1710Z on 8 December 1998 were analyzed. The receivers were allowed to operate for the first 30 minutes with no jamming. The aim of Test 7 was to investigate the impact of jamming at L1 at various jamming levels. Jamming was on for two or three minutes followed by eight minutes of no jamming allowing the receiver to regain lock. The attenuator was set at four different levels 85, 80, 75 and 70 dB resulting in J/S of 20.7, 25.7, 30.7, and 35.7 dB (Table 4.1) as shown in Figure O.18.

An overview of the satellite constellation status is provided in Figures O.1 and O.2 and the satellite PRN numbers used in the navigation solution in Figure O.3. Figure O.4 relates the satellite PRNs being tracked by each receiver channel and Figures O.12 to O.17 indicate the C/N_0 for each of the tracking channels. Channel 11 was idle throughout the test. GDOP values typically ranged between 2 and 5 over the first 110 minutes. At minute 110 GDOP spiked to 24 (Figure O.5).

As shown in Figure O.6, the effects of various levels of jamming on the Doppler frequency offset can be seen at minutes 30, 40, 50, 60, 80, 90, 100, and 110. A general lowering of the C/N_0 levels can also be seen at these times in Figures O.12 to O.17. From the C/N_0 plots it can also be seen that when the tracking channels lock on to the CW, the C/N_0 demonstrates a fairly constant value during each jamming window. In some cases the plots indicate a higher C/N_0 for higher jamming levels such as for channel 2 in Figure O.12 at minute 60 and 110.

At minute 30 a small ripple is seen in the Doppler frequency offset plot, shown in Figure O.7, for PRN 8 (channel 3 from Figure O.4). Channel 3 broke lock momentarily as shown in the C/N_o plot of Figure O.13 for channel 3. Although it did not lose lock at minute 40 even though the jamming level was 5 dB higher, the lowering of C/N_o was still evident in Figure O.13 for channel 3. At minute 50 and minute 60, PRN 8 (channel 3) locked on to the jamming signal at -3994 Hz as shown in Figure O.7. The locking on to the CW is evident in the C/N_o plot for channel 3 in Figure O.13 as the C/N_o actually increased during the two minute jamming periods at minute 50 and minute 60.

At minute 50 and 60, PRN 5 (channel 2) locked on to the CW jammer (Figure O.7) at -2994 Hz and exhibited similar characteristics in Figure O.12 for channel 2 as previously shown for channel 3. At minute 60, PRN 14 (channel 4) and PRN 25 (channel 8) were also locked on to the CW jammer (Figure O.7) at 3006 Hz and 6 Hz respectively.

From the C/N_o plots of Figures O.12 to O.17 it can be seen that PRN 1 (on channel 1 and 12) and PRN 21 on channel 6 were the only two satellites not to lose lock due to the jamming. A dip in C/N_o values to 37 dB-Hz and 30 dB-Hz occurred for the two PRNs respectively at minute 63. From the C/N_o plots it appears that had the jamming been sustained for a longer duration that both of these PRNs would have broke lock.

At minute 80 receiver channel 7 ceased attempting to track PRN 23 and attempted to track PRN 22 (Figure O.4). The Doppler frequency offset plot of Figure

O.8 highlights the tracking channels for PRN 22 (channel 7), and PRN 5 (channel 2) after the jamming ceased at minute 82. PRN 22 regained lock at minute 88 and PRN 5 regained lock at minute 83 but because the satellites were low on the horizon they were more susceptible to losing lock. At minute 90, PRN 22 did not lock on to the CW but PRN 5 did (PRN 22 was increasing in elevation angle while PRN 5 was decreasing). At minute 92, although the jamming had ceased, the receiver continued fixed at -2990 Hz until the jamming commenced again at minute 100, when PRN 5 locked on to -4990 Hz. At minute 110 channel 2 ceased to attempt tracking on PRN 5, switched to PRN 6 and immediately locked on to the jamming. PRN 22 locked onto the CW jammer at 3011 Hz. The effects on C/N_0 are highlighted in Figure O.15 for PRN 22 on channel 7 and in Figure O.12 for PRN 5 on channel 2.

The increase in position error at minutes 50, 60 and 110 are shown in Figures O.9 and O.10. At minutes 50 and 60, PRN 5, which was locked on to the CW signal, was used in the navigation solution (Figure O.3) and corresponded to the increase in position error to a maximum of 4.05 km and 12.33 km for the two respective times. The receiver reported the error of 4.1 km as a valid 3D fix at minute 52; however, at minute 61.8 the receiver flagged the error as invalid by the time the error had grown to 6.8 km.

At minute 100, PRNs 1, 14, 21, 25 and 29 were used in the navigation solution; none of which were locked on to the CW signal and hence no dramatic increase in position error occurred for this jamming window. Between minute 110 and 112 during the last jamming window, both PRN 22 and PRN 30 (locked on to the CW jamming

Figure O.8) were used in the navigation solution and resulted in an increase in position error to 5.6 km (Figure O.10). The receiver continued to report this as a valid position.

4.6.6 TEST 8 RESULTS (FIGURES CONTAINED IN APPENDIX P)

Data collected at a rate of one sample per second for Test 8 between 1510Z and 1710Z on 11 December 1998 were analyzed. The receivers were allowed to operate for the first 20 minutes with no jamming. Since low elevation satellite signals are generally more susceptible to interference, the aim of Test 8 was to investigate the impact of jamming at L1 at various jamming levels and to investigate the concept of increasing the elevation mask angle to 25 degrees in order to remove low elevation jammed satellites from the navigation solution. Jamming was on for two minutes followed by three minutes of no jamming allowing the receiver to regain lock. The attenuator was set at four different levels 85, 80, 75 and 70 dB resulting in J/S of 20.7, 25.7, 30.7, and 35.7 dB as shown in Figure P.19.

An overview of the satellite constellation status is provided in Figures P.1 and P.2 and the satellite PRN numbers used in the navigation solution in Figure P.3. Figure P.4 relates the satellite PRNs being tracked by each receiver channel and Figures P.13 to P.18 indicate the C/N_0 for each of the tracking channels. Channels 6, 10, and 11 were idle throughout the test. GDOP values were higher than previous tests since the available number of satellites were limited by the increased elevation angle. GDOP typically ranged between 3 and 5 over the first 50 minutes. GDOP spikes occurred at minute 60, 65, 67, and minute 70 with values of 126, 89, 78, and 23 respectively (Figure

P.5). The spike in GDOP to a value of 1000 at minute 92 was associated with the receiver switching from a 3D fix to a 2D fix, but the receiver quickly regained 3D fix status within seven seconds. The large vertical spikes of C/N_0 as a result of the jamming are highlighted for PRN 1 on channel 1 in Figure P.13 and channel 12 in Figure P.18.

At the beginning of data capture, PRN 5 (on channel 2) was already slightly below the 25 degree elevation angle and at minute 10, PRN 5 ceased to be tracked by the receiver at an elevation angle of 20 degrees and Doppler frequency offset was set at a constant value. PRN 5 (channel 2) locked on to the CW jammer at -4073 Hz at minutes 20 and 25, - 3068 Hz at minute 30 and -5070 Hz at minute 35. The effects of CW jamming on PRN 5 are highlighted in Figure P.13 for channel 2 for the first 37 minutes of the plot. The wide swaths generated by PRN 5 were a result of the receiver channel searching once the jamming was switched off. It should be noted that between minute 40 and 50, PRN 5 (channel 2) was not locked on to the jammer but demonstrated constant Doppler frequency. This was attributed to the fact that the receiver would recognize that the satellite was below the elevation mask angle once it attempted to regain lock using previous ephemeris/almanac data (Figure P.7).

At minute 20, PRN 8 ceased to be tracked as the elevation angle passed below 25 degrees and is shown in Figure P.14 for channel 3. At minute 35, PRN 25 on channel 7 locked on to the CW jammer at -70 Hz for two minutes as shown in Figure P.7. Since PRN 25 was used in the navigation solution, an increase in position error up to 1.28 km resulted as noted in Figure P.10 for minute 35.5 to 37. Between minute 65.2

and 67.2 position error increased to a maximum value of 11.75 km (Figure P.11) as a result of PRN 30 on channel 9 being locked on to CW jammer (Figure P.8) and being used in the navigation solution. Channel 9 regained lock on the valid PRN 30 once the jamming was removed and as a result the large position error was removed. The XR5-M receiver reported that the GPS 3D fix was valid even though position errors had grown to 1.28 and 11.75 km for the above two periods (Figures P.10 and P.11).

At minute 90 channel 3 commenced attempting to lock on to PRN 22 but locked on to the CW jamming instead at 2945 Hz as shown in Figure P.9. The wide frequency swath between minute 92 and 95 is the receiver searching for PRN 22. At minute 95 while channel 3 was still searching for PRN 22 the channel locked on to the CW jamming at 946 Hz. Channel 3 finally gained lock on PRN 22 at minute 97 once the jamming ceased.

During Test 7 the jamming of PRN 5 resulted in an increased position error. The increase in elevation mask angle to 25 degrees during Test 8 prevented PRN 5 from being used in the navigation solution even though it was locked on to jamming signal and resulted in improved position measurements during jamming windows compared to Test 7.

4.7 SWEPT CW TEST RESULTS

This section discusses the results of swept CW jamming conducted in Test 9-11 and the respective figures are contained in Appendix Q, R and S.

4.7.1 TEST 9 RESULTS (FIGURES CONTAINED IN APPENDIX Q)

Data collected at a rate of one sample per second for Test 9 between 1500Z and 1700Z on 6 December 1998 were analyzed. The XR5-M receivers were allowed to operate for the first 30 minutes with no jamming. The aim of Test 9 was to investigate the impact of swept CW jamming centered at L1 at five jamming levels, and for three frequency spans (2 MHz, 200 kHz, and 20 kHz). Sweep time of the signal generator was set to 20 seconds. Jamming was on for two minutes followed by three minutes of no jamming allowing the receiver to regain lock. The attenuator was set at five different levels 85, 80, 75, 70, and 65 dB resulting in J/S of 20.7, 25.7, 30.7, 35.7, and 40.7 dB as shown in Figure Q.20.

An overview of the satellite constellation status is provided in Figures Q.1 and Q.2 and the satellite PRN numbers used in the navigation solution in Figure Q.3. Figure Q.4 relates the satellite PRNs tracked by each XR5-M receiver channel and Figures Q.14 to Q.19 indicate the C/N_0 for each of the tracking channels. Channel 11 was idle throughout the test with one exception at minute 80 (during the highest jamming level). GDOP values typically ranged between 2 and 4 over the first 35 minutes. Large GDOP spikes were associated with the swept CW jamming windows (Figure Q.5). The large vertical spikes in C/N_0 as a result of the jamming are evident in Figures Q.14 to Q.19.

The large dark vertical swaths in Figure Q.3 are a result of the receiver rapidly changing the satellite PRNs used in the navigation solution. This was a result of the jammer sweeping through the tracking channels and rapidly causing the tracking channels to break and regain lock on the satellite signals. The highest jamming levels

commenced at minute 50, 80, and 110. From Figure Q.4 it can be seen that the receiver did a complete reset of assigned PRNs to the tracking channels at minute 80.

During the pure CW jamming in Tests 3 to Test 8, the receiver locked on to the jammer for long periods of time as evident in the long horizontal lines in the Doppler frequency offset plots. From the Doppler frequency offset Figures Q.7 and Q.8 the large vertical spikes in frequency, which result from the swept CW jamming, are evident as jamming commences at minutes 40, 45, 50, 65, 70, 75, and 80. The magnitude of vertical deflection generally increases as the jamming level increases. Once the jamming ceased, the areas of vertical deflection indicated the XR5-M receiver searching to regain lock. Because the tracking channels were pulled off frequency by a large amount during the jamming, the receiver channels were unable to reacquire the actual GPS signal once jamming ceased. As a result, the tracking channels remained in reacquire mode for up to three minutes until the next jamming window which then pulled the tracking channel frequencies off even further in frequency (Figure Q.9).

Perhaps the most interesting aspect of the swept CW jamming compared to results of Test 3 to Test 8 are the relatively small position errors as shown in Figures Q.11 and Q.12. The jamming at minute 50 to 52 caused the receiver to lose lock and the 3D position error increased to only 24.7 meters. Other examples of rather small position errors for minutes 75.8, 101.6, 105.2, and 112.2 were 102.0, 77.8, 49.2 and 19.3 meters respectively.

From the results it can be seen that the highest swept CW jamming levels of J/S of 40.7 dB during Test 9 caused the receiver to cease providing valid navigation data.

The receiver underwent rapid loss of carrier and code lock and was forced to reacquire the satellite as a result of the jamming. For the center frequency, frequency span, and sweep width used in this test, the position errors were relatively small compared to the position errors from pure CW jamming results of Test 3 to Test 8. There was one exception to the position error observations with a spike at minute 82 after the complete channel reset shown in Figure Q.4.

4.7.2 TEST 10 RESULTS (FIGURES CONTAINED IN APPENDIX R)

Data collected at a rate of one sample per second for Test 10 between 1500Z and 1710Z on 7 December 98 were analyzed. The receivers were allowed to operate for the first 30 minutes with no jamming. The aim of Test 10 was to investigate the impact of swept CW jamming centered at L1 at four jamming levels, and for two different frequency spans (20 kHz and 10 kHz). The sweep time on the signal generator was set to 20 seconds. Jamming was on for two minutes followed by eight minutes of no jamming allowing the receiver to regain lock. There is a no jamming period of 18 minutes between minute 62 and minute 80 to allow the receiver to regain lock and avoid any impact on the next jamming period. The attenuator was set at four different levels 85, 80, 75, and 70 dB resulting in J/S of 20.7, 25.7, 30.7 and 35.7 as shown in Figure R.18.

An overview of the satellite constellation status is provided in Figures R.1 and R.2 and the satellite PRN numbers used in the navigation solution in Figure R.3. Figure R.4 relates the satellite PRNs being tracked by each receiver channel and Figures R.12

to R.17 indicate the C/N_0 for each of the tracking channels. Channel 11 was idle throughout the test. GDOP values typically ranged between 2 and 4 over the first 50 minutes with one jump at minute 31 up to a GDOP of 23 as shown in Figure R.5. From Figure R.3 jamming at minute 30, 40, 50, 60, 80, 90, 100, and 110 results in the receiver assigning different combinations of five PRNs to the navigation solution. Large GDOP spikes were associated with the higher swept CW jamming levels at minutes 50, 60, 100, and 110 (Figure R.5). The large vertical spikes of C/N_0 , as a result of the jamming, are evident in Figures R.12 to R.17.

The receiver ceased calculation of positional information intermittently at minute 60 to 63 and between minute 110 and minute 114. GDOP values were reported as 2000 for these periods of positional information outages. These outage windows were associated with the highest jamming levels during this test. As shown in the Doppler plot in Figure R.8, with the start of jamming at minute 110, eight of the tracking channels were pulled off. For the next eight minutes the tracking channels attempted to reacquire. PRNs 25 and 15 regained lock allowing a valid navigation solution to be achieved; however, PRNs 14, 1, 22, 29 and 30 remained in reacquire mode until minute 120 when all the channels finally regained lock. This same observation was noted on PRN 14 in Figure R.7, when PRN 14 was jammed at minute 60-62 and was in reacquire mode for eight minutes until it regained lock at minute 70. It would appear from this that the XR5-M receiver was designed to remain in the reacquire mode for at least eight minutes. Similar results were obtained as shown in Figure R.8 for jamming from minute 100 to minute 102. After the jamming was

removed at minute 102, PRNs 14, 22, 30, 15, and 5 remained in reacquire mode until jamming was turned on again at minute 110 and the channels were again pulled off to the jamming signals. These results reinforce the concept that more than eight minutes should be allowed for the XR5-M receiver to regain lock prior to conducting another jamming window. As a result of using the eight minute time frame between jamming windows, the results of the window from minute 110 to 120 are biased from the previous jamming window of minute 100 to minute 102. Future testing should account for more than eight minutes between test windows to allow all the XR5-M receiver channels to regain lock.

In terms of position errors, at minute 110, the receiver broke 3D fix status, but the 3D position error was less than 30 meters (Figures R.9 and R.10). The worst case position error of approximately 220 meters for this test resulted at minute 60 (Figure R.9). This error was reflected in the change in receiver clock drift rate as shown in Figure R.11 at minute 60.

Figures R.12 to R.17 highlight the effects of the swept CW on the C/N_0 values. From Figure R.4 the receiver tracking channel 1 was tracking PRN 1 and channel 9 was tracking PRN 29. The C/N_0 for PRN 1 (channel 1 Figure R.12) and PRN 29 (channel 9 Figure R.16) highlight the effects of the two minute jamming windows at minutes 30, 40, 50, 60, 80, 90, 100, and 110. As the levels of jamming were increased from minutes 30 to 62 and from minutes 80 to 112 the C/N_0 values were pulled down during each of the two minute windows. At the jamming level at minute 60 and 110, the C/N_0 was reduced to zero. Other channels displayed similar characteristics of reduced C/N_0 .

values. At the same times high intermittent peaks in C/N_0 occurred as the receiver tracking channels locked on to the jamming signal; values exceeding 50 dB-Hz were observed during the jamming windows.

For the time period used for testing, the Doppler frequency values typically ranged from +3.1 kHz to -4.9 kHz. This bias in Doppler frequency offset is discussed in greater detail in Section 4.9.1. From minute 100 to 102, the swept CW pulled PRN 14 off to 20 kHz (Figure R.8). The change in tracking frequency depends on the combination of the sweep time and the sweep width. The jamming signal must dwell for a sufficient amount of time within the tracking channel bandwidth to capture the tracking loop. No assessment was made of different center frequencies for the swept CW tests. The frequency span was 20 kHz for the four jamming periods between minute 30 and 62, while the frequency span was 10 kHz for the four jamming periods between minute 80 and 112. Comparing the results for the two different frequency spans for Figure R.7 and Figure R.8 it would appear that the narrower frequency span of 10 kHz actually was more effective in pulling the tracking channels off a greater distance from the actual tracking frequencies. It must be remembered that the incoming jamming signal is spread by the receiver generating a moving array of 1000 Hz spectral lines that are sweeping through the tracking bandwidth of the receiver.

4.7.3 TEST 11 RESULTS (FIGURES CONTAINED IN APPENDIX S)

Data collected at a rate of one sample per second for Test 11 between 1500Z and 1710Z on 10 December 1998 were analyzed. The receivers were operated for the first

30 minutes with no jamming. The aim of Test 11 was to investigate the impact of swept CW jamming centered at L1 at five jamming levels, and for three different frequency spans (2 MHz, 200 kHz and 20 kHz) at a sweep rate of one second. Jamming was on for two minutes followed by three minutes of no jamming allowing the XR5-M receiver to regain lock. The attenuator was set at five different levels 85, 80, 75, 70 and 65 dB resulting in J/S of 20.7, 25.7, 30.7, 35.7, and 40.7 dB as shown in Figure S.19.

The original Test 11 scenario was designed to maintain similar jamming windows so that a comparison of the results of Test 9 with a sweep time of 20 seconds could be made to Test 11 with a sweep time of one second as shown in Table 4.2. It is recommended that Test 9 and Test 11 be repeated with no jamming windows of more than eight minutes between jamming windows, based on the results of Test 10.

An overview of the satellite constellation status is provided in Figures S.1 and S.2 and the satellite PRN numbers used in the navigation solution in Figure S.3. Figure S.4 relates the satellite PRNs being tracked by each receiver channel and Figures S.13 to S.18 indicate the C/N_0 for each of the tracking channels. Channel 11 was idle throughout the test. GDOP values typically ranged between 2 and 5 over the first 50 minutes. As shown in Figure S.3, jamming at minute 51, and 101 resulted in the receiver rapidly assigning different combinations of five PRNs to the navigation solution. The large GDOP from minute 110 to 112 was associated with the receiver losing lock (Figure S.5) and was reflected in the position error frozen in Figure S.11 for the same period. The large vertical spikes of C/N_0 , as a result of the jamming, are evident in Figures S.13 to S.18.

The five jamming windows between minute 30 and 52 were associated with a two MHz frequency span at a sweep time of one second. From Figure S.7, it can be seen that as the jamming level is increased for each window, the jamming pulls more channels off frequency. At the maximum jamming level at minute 50 to 52, PRNs 14, 15, 5, 8 and 23 are all pulled off carrier lock. The C/N_0 plots for channels 10, 4, 2, 3, and 6, respectively, highlight the reduction in C/N_0 .

The jamming windows for the periods minute 60 to 82 and minute 90 to 112 demonstrate an interesting characteristic as seen in Figures S.8 and S.9. During the two minute jamming windows, the Doppler frequency offset appears to remain relatively constant, similar to the pure CW jamming effects from Tests 3 to Test 8. The pulling off of the Doppler frequency for PRN 22 only results after the tracking channel has entered reacquire mode and then relocks on to the jamming at the beginning of the next jamming window. From the C/N_0 plot for Figure S.15 channel 6 (PRN 22) it can be seen that the tracking channel remains locked on to the jamming signal during jamming windows for minute 90 to 92, 95 to 97, 100 to 102, 105 to 107, and 110 to 112.

The spectral characteristics of 1000 Hz lines in the swept CW jamming are evident at minute 110 in Figure S.9. PRN 22, 14, 6, and 29 locked on to 9950, 1950, 950 and -2050 Hz respectively. PRN 1, 15, and 30 locked on to -3050 Hz, and PRN 21 locked on to -5050 Hz. Similar examples of the 1000 Hz spreading are evident in Figures S.8 and S.9 for other jamming windows.

The impact of swept CW jamming on position error is reflected in Figures S.10 and S.11. The largest position error was 122.0 meters and occurred at minute 81.5. The

relatively small position error was correlated with the small change in the XR5-M receiver clock drift rate with one small spike at minute 81.5, as shown in Figure S.12.

4.8 CW JAMMING IMPACT ON POSITION ERROR

This section was dedicated to the investigation of position error as a result of CW jamming. Figures for Test 12 are included in Appendix T.

4.8.1 TEST 12 RESULTS (FIGURES CONTAINED IN APPENDIX T)

Data collected at a rate of one sample per second for Test 12 between 1430Z and 1705Z on 17 December 1998 were analyzed. The receivers operated for the first five minutes with no jamming. The aim of Test 12 was to investigate the magnitude of position error as a result of pure CW jamming centered at L1 at a single jamming level. Jamming was on for ten minutes followed by five minutes of no jamming allowing the receiver to regain lock. The attenuator was set at 70 dB resulting in a J/S of 35.7 dB versus time as shown in Figure T.22.

Based on the results of Test 10, and observations in this test, future testing should ensure that more than eight minutes are allowed between jamming windows to prevent jamming windows from creating a potential bias from previous jamming windows. An example of this is shown in Figure T.8. PRN 22 was locked on to the jamming at minute 70. Jamming ceased at minute 75 and the tracking channel attempted to reacquire. Five minutes later the jamming commenced and immediately the tracking channel locked on to the jamming signal. Similar characteristics of PRN 5

were observed during the first 50 minutes of the test. Although the potential existed to generate a bias from one test window to the next, the effect on Test 12 was minimal since PRN 5 was not used in the navigation solution during the first 50 minutes of the test. Additionally, PRN 22 was not used in the navigation solution until after it gained a valid lock at minute 136.

There were a total of 10 jamming windows of 10 minutes each as shown in Figure T.22. Five minutes of no jamming allowed the receiver to regain 3D fix status prior to the start of the next jamming window as evident in the position error plots as shown in Figures T.11 and T.12. The ten jamming windows resulted in ten windows of position error growth as shown in Figures T.11 and T.12.

An overview of the satellite constellation status is provided in Figures T.1 and T.2 and the satellite PRN numbers used in the navigation solution in Figure T.3. Figure T.4 relates the satellite PRNs being tracked by each receiver channel. Figures T.16 to T.21 indicate the C/N_0 for each of the tracking channels. Channel 11 was idle throughout the test. GDOP values typically ranged between 2 and 5 over the first 50 minutes as shown in Figure T.5. Spikes in GDOP to 1000 were evident at minutes 60, 105, 125, 135 and 140. One spike in GDOP to 2000 occurred at minute 150.

An expansion of the Doppler frequency offset is provided in Figure T.7. Channel 3 attempts to lock on to PRN 5 prior to jamming during the first five minutes of the run. Once the jamming commences at minute 5, channel 3 (PRN 5) locks on to the CW signal. Channel 2 (PRN 8) and channel 5 (PRN 23) lock on to the jamming signal within the first few minutes. At minute 10, channel 10 (PRN 15) and channel 7

(PRN 25) lock on to the CW jamming. At minute 15, jamming ceases and channel 3 attempts to reacquire which generates the wide vertical swaths in Figure T.7. The C/N_o plot in Figure T.17 for channel 3 (PRN 5) highlights the receiver channel tracking the jamming signal followed by no signal periods.

From the Doppler frequency plots of Figures T.6 through T.9, it can be seen that channels 1 and 12 (which are tracking PRN 1) do not lock on to the jamming during the entire test. From the C/N_o plots in Figure T.16 (channel 1) and Figure T.21 (channel 12) the C/N_o is reduced during the jamming windows but not enough to cause the tracking channel to lock on to the jamming signal.

At minute 20, jamming commences and quickly locks up PRNs 5, 8, and 23 (channels 3, 2, and 5 respectively). At minute 24, PRN 30 (channel 8) locks on to the jamming signal. The four channels remain locked until jamming ceases at minute 30 (Figure T.7). At minute 35, PRNs 8 and 23 lock on to the jamming signal at -4063 Hz, while PRN 5 locks on to jamming at -5063 Hz. From minute 10 to minute 40, channel 9 is assigned to PRN 16. The C/N_o plot in Figure T.20 shows that channel 9 is not locked on to any signal during this window. At minute 40, channel 9 is reassigned to PRN 14 and immediately locks on to the jamming (Figure T.7). At minute 50, PRNs 5, 8, 14, and 25 (channel 7) are locked on to the jamming signal. PRN 23 locks on to the jamming at minute 53. At minute 65, PRNs 5, 8, 23, 15 are locked on to the jamming signal. Five minutes later channel 5 is reassigned from PRN 23 to PRN 22 and locks on to the jamming. PRN 14 also locks on to the jamming at minute 70. Similar results of the tracking channels locking on to the jamming signals can be seen during jamming

windows in Figure T.9. In particular jamming between minute 125 and 135 results in PRNs 22, 6, 14, 30, 15, and 21 all locking on to the jamming signal.

Position error is highlighted in Figures T.11 to T.14. The large position error evident in Figure T.11 (due to scale of the plot) masks the position error for each of the jamming windows in Figures T.12 and T.14.

Figure T.10 provides an indication of the receiver status; a value of two indicates that the receiver has "3D FIX" status, a value of one indicates the receiver fixing is based on "2D FIX" status, and a value of zero indicates that the receiver has "NO VALID FIX". There were 13 events when the receiver switched from having a valid fix to the "NO VALID FIX" status during this test. For each of these events, position error was measured and is provided in Table 4.5. The position error had a mean of 12.492 km and a standard deviation of 6.565 km. Maximum position error at the second prior to losing a valid fix was 22.999 km and the minimum was 3.730 km.

The position error plots of Figure T.11 to Figure T.14 include the position error calculated after the receiver flags the position as no longer valid. This data was provided in all position error plots to offer insight into what actually happened within the receiver during the NO VALID FIX periods.

4.9 SPECIAL OBSERVATIONS

This section discusses particular observations over the course of the six weeks of testing. Some subjects did not merit further discussion in this section but were included in Appendix H as a summary of lessons learned.

Time (seconds)	Position Error (meters)
593	22,264
684	17,183
2406	10,586
3204	15,551
3247	17,220
4045	6,881
4233	16,269
5003	5,938
6123	3,730
6201	5,123
7564	6,663
7597	11,989
8448	22,999

Table 4.5 - Position Error as Result of CW Jamming

4.9.1 BIAS IN DOPPLER FREQUENCY OFFSET

An interesting observation was the overall negative bias or shift in all of the Doppler frequency plots. Given the HP spectrum analyzer used, it was not possible to measure the frequency output of the signal generator to a fine resolution of a few Hertz. The first two weeks of testing were used to determine the bias in the signal generator by comparing the output to Doppler frequencies that were jammed. This bias was originally estimated at -150 Hz. All values in Tables 3.1 to 3.4, and Table 4.2 were based on output frequencies corrected for this bias. The overall bias in the Doppler frequency was first believed to be associated with satellite orbit and GPS receiver relative velocity shifts. Upon further analysis, the bias in the Doppler frequencies was associated with the receiver clock drift rate. The receiver clock drift rate observed during the tests was approximately 5.6×10^{-7} seconds/second and equates to 167.9

meters/second. Using 5.255 Hz per meter/second of Doppler shift at L1 results in an approximate shift of 882 Hz in the negative direction. This explains the overall negative shift in Doppler frequencies to a range between approximately +3.1 kHz and -4.9 kHz.

Once corrected for this bias the Doppler frequency offsets would be approximately ± 4 kHz. Although GPS Doppler shift is reported as approximately ± 6 kHz [PAR96] for a stationary user at the earth's surface, this maximum value is limited to latitudes above approximately 50 degrees. For a latitude of 40 degrees (ie. AFIT) the maximum Doppler shift from a GPS satellite is approximately ± 4 kHz for a stationary user at the earth's surface, which was consistent with the results observed.

Another small apparent bias was related to the elevation angle for gaining and losing lock. Receiver channels that have signal lock tend to remain locked to lower levels of C/N_0 and hence lower satellite elevation angles than for initial acquisition. This accounts for a very slight difference between the magnitude of the Doppler shifts at the gaining and losing lock points when there is no jamming present.

This research has shown that it is feasible to selectively jam a satellite using the Doppler frequency offset in the laboratory environment and that the technique may be of benefit in an operational environment. In the future, "smart jamming" systems can take advantage of the maximum amplitude spectral lines and Doppler shifted frequencies of each satellite PRN code in order to jam C/A code GPS receivers.

4.9.2 WAVE IN DOPPLER FREQUENCY OFFSET

During the first few minutes of data capture during the pre-test periods, a wave in the Doppler frequency offset was observed. This effect was avoided by allowing the receivers to operate for approximately fifteen minutes prior to capturing data. Two examples of not waiting the full period demonstrate this wave in Doppler frequencies. The change in receiver clock drift rate is associated with the change in Doppler frequencies during first few minutes of operation, as seen in Figures L.6 and L.12 and to a lesser extent Figures S.6 and S.12.

4.9.3 INTERMITTENT LOSS OF LOCK ON PRN 15

The loss of lock on PRN 15 in Test 2 was initially discussed in Test 2 results. During Test 2 there was no jamming and no receiver channel seemed to exhibit a decrease in C/N_0 , as might have been expected for an unexpected RF interference source. Additionally, the loss of lock was not preceded by a short duration pulling of the frequency as was typical for CW jamming. Based on these observations and because there was no intentional jamming present, this was probably due to a problem specific to PRN 15 and caused by some rapid form of interference which was not of RF origin. Further looking at the azimuth (275 degrees true) and the elevation angle (26 degrees) at the time of loss of lock suggest possible masking of the GPS antenna by AFIT Building 640 rooftop superstructure (Appendix A). This is a weak explanation given that the incident was not observed on any other test during the six weeks of

testing. The cause of this loss of lock for a 5 second duration on three occasions remains unexplained.

4.9.4 MULTIPATH EFFECTS

Multipath effects on PRN 14 were observed during several tests including Test 1, 2, 5, and 6. The multipath effects were also observed during other tests; however, jamming interference impacted the multipath effects. The replacement of the two volute antenna with two choke ring antenna is recommended to reduce the multipath effects for future testing purposes. Using a single antenna with two receivers should allow the multipath effects to be removed since the errors would be common to both receivers.

The periodic increase and decrease in C/N_0 is a characteristic of multipath effects observed at low satellite elevation angles. As the multipath signals change in phase with the relative change in path lengths due to the relative motion of the satellite and the user, the C/N_0 increases and decreases periodically as a function of this phase shift. Numerous examples of this were observed in the C/N_0 plots for low elevation satellites throughout the tests.

4.9.5 JAMMING USING STRONG SPECTRAL LINE CHARACTERISTICS

Offsetting of the jamming center frequency to match the strongest spectral line of a given PRN code may be used to selectively jam a specific satellite as was observed with PRN 30 in Test 6 at a moderately low J/S of 25.7 dB for the XR5-M receiver. The

technique is limited to the jamming of C/A code receivers. Conceptually, several jammers could be co-located each targeting the strongest spectral line for each PRN code. In the future smart CW jammers may be optimized to jam specific satellites for a given location and time of day. Based on initial positive results using the XR5-M receiver, the concept of selectively jamming a received satellite signal by using a combination of the required Doppler shift and a maximum spectral line for each PRN code merits further study. Similar testing using other PRN codes and other C/A code receivers is recommended.

4.10 DEVELOPMENT OF GPS JAMMING TRAINING

Several options exist for the development of dedicated "hands-on" GPS jamming training. A homework assignment may be generated using the data (in MATLAB[®] format) collected during this thesis. Students could conduct an analysis using the "sptool" graphical user interface found in the MATLAB[®] signal processing toolbox using actual data from the thesis. This would require a minimum knowledge of MATLAB[®] and minimum preparation effort based on analysis already conducted. A new set of data could also be collected, tailored, and provided to the students for analysis.

A more advanced lab would require students to conduct actual GPS jamming scenarios. This would offer a much more rewarding option for graduate students. The 746th Test Squadron at Holloman, AFB, is one of the recipients of AFIT graduates, especially from the Navigation and Controls sequence. The opportunity to use

hardware including GPS receivers, an HP Signal Generator, an HP Spectrum Analyzer and an HP Variable Attenuator would be extremely beneficial in the students' follow-on assignment. At least four laboratory hours should be dedicated to each group of students. The first hour would be used as an equipment orientation, two hours would be used to capture data at various jamming levels and jamming types, and the final hour would be used to manipulate the data file into a useable text file and commence data analysis.

A symbol file specifically designed to the lab could be generated or selection of one of several symbol files already generated and installed on the 486 PCs could be used depending on the level of detail required and the amount of MATLAB[®] coding required of students. It is further recommended that the students use the symbol file <kdsymb13.sy> that is highlighted at Appendix C.

Finally, it is recommended that a jamming lab be preceded by a lab assignment using the XR5-M receiver in non-differential mode. The jamming lab should use the differential setup used during this thesis work. This would provide students a feel for how differential techniques can be used to remove errors correlated between the two receivers. A more advanced assignment could be used in which students would use the XR5-M as an actual mobile receiver and would be required to generate specific MATLAB[®] code in order to conduct single and double difference techniques.

On a slightly different note, but along the thoughts of training of jamming of GPS, the following comment is offered. Currently, the Canadian Forces (CF) lacks GPS jamming training devices for use during exercises. Also of concern is the impact of the jamming of GPS on civil GPS users. Perhaps one of the simplest modifications

for use in a maritime environment would be the modification of sonobuoys to transmit jamming signals. The sonobuoy could be modified/designed as a miniature low power GPS jammer for use at sea. A simple design could simply transmit a CW signal at L1. More advanced designs would allow the user to program frequencies, pulse rates, and even PRN codes. The use of GPS jammers at sea would also reduce the interference to land based civilian users of GPS. The subject merits further investigation to meet anticipated future needs for Navigation Warfare in the CF and could represent an ideal thesis topic for future students at AFIT, the Naval Post Graduate School in Monterey, California, or the Royal Military College in Kingston, Ontario, Canada.

4.11 CHAPTER SUMMARY

The final equipment configuration used for Tests 1 to 12 is suitable for the future instruction of jamming of C/A code GPS receivers. An ability to generate and measure a jamming signal very accurately is highly desired. No measurements of actual antenna and pre-amplifier gain were conducted. The impact of wideband noise and pulsed CW on the XR5-M receiver was not investigated.

Although the Doppler frequency has a larger magnitude at lower elevation angles, the rate of change of Doppler frequency is smaller at lower elevation angles. Because of this, CW jamming signals will dwell for a longer period of time as the frequency of the tracking channels for low elevation satellites moves through the jamming window. In addition, satellites at low elevation had lower C/N_0 , making them

more susceptible to jamming signals. In particular, PRNs 5, 8, 14 and 22 regularly locked on to the CW jamming signal in Tests 3 to 8.

The success of selectively jamming PRN 30, in Test 6, by offsetting the frequency of the CW jammer to target the maximum strength spectral line of PRN 30 merits further investigation based on initial results. It is feasible that a set of CW jammers each targeted to specific satellites could prove to offer more effective CW jamming techniques. In the electronic warfare world of counter moves, this may suggest future research into the design of filters optimized for this particular set of jamming frequencies.

A summary is provided in Table 4.6 for position error in the ECEF coordinate system for Test 1 and 2 (for the case of no jamming). The method used in calculating these values was discussed in Section 4.5.1.

	TEST 1	TEST 2
Mean Error in ECEF "X" Direction (meters)	-0.365	-0.292
Mean Error in ECEF "Y" Direction (meters)	0.0937	-0.428
Mean Error in ECEF "Z" Direction (meters)	-0.757	0.987
Mean of 3D Error (meters)	6.923	5.848
Standard Deviation of 3D Error (meters)	4.293	3.112

Table 4.6 - Summary of No Jamming Results for Tests 1 and 2

Multipath effects contributed to the position error given the superstructure on the AFIT Building 640 rooftop and the use of volute antenna. The magnitude of the mean position error for both Test 1 and Test 2 was greatest in the Z direction.

In general terms, CW jamming generated much larger position errors prior to the XR5-M setting the no-valid-fix flag while swept CW generated relatively small position errors prior to the no-valid-fix flag being set.

Results of Tests 3 to 8, and Test 12, indicated that CW jamming caused the tracking channels to actually lock on to the jamming signal. Position errors as a result of CW jamming reached a mean of 12.492 km and a standard deviation of 6.565 km prior to being flagged as an invalid fix during Test 12. Maximum position error at the second prior to losing a valid fix was 22.999 km and the minimum was 3.730 km. Position error plots of for all test results include the error in position as the receiver continues calculating navigation information after it has flagged the position output as invalid. This provided insight into the magnitude of position errors as result of jamming before the XR5-M receiver regained valid fixing status.

CW jamming, with J/S of 20.7 to 35.7 dB, was investigated during Test 3 to 8. Even the relatively low J/S of 20.7 dB during Test 3 rendered the receiver output invalid given a long enough period for each of the tracking channels to acquire the jamming signal (Figure K.6). Between minutes 74 and 84 for Test 3, 3D position error rapidly grew (Figure K.11) as a result of only one jammed satellite in the navigation solution (PRN 5 in Figure K.7).

The higher J/S of 35.7 dB during Test 5 captured more of the XR5-M receiver channels in a shorter timeframe, as was evident in the jamming results commencing at minute 80 (Figure M.6). Position error rapidly increased and the receiver ceased to output navigation information by minute 100. The two minute spiking in the C/N₀ and Doppler offset frequency after minute 100 was attributed to a two minute time-out that caused each of the tracking channels to reset when the channels were unable to synchronize to the data frame within that period [BUT99].

The XR5-M receiver encountered difficulty in acquiring PRN 5, as was evident for several minutes at the beginning of Tests 1, 6 and 12. At low elevation angles, PRN 5 and PRN 8 routinely locked on to the jamming signal throughout the test period. By raising the elevation angle to 25 degrees in Test 8, PRN 5 was removed from the navigation solution preventing an increase in position error from PRN 5.

There is obviously a trade-off to be made by the user between increasing GDOP and hence position error in the absence of jamming by increasing the elevation mask angle. The concept was intended as a potential quick fix for fielded C/A code GPS receivers. The technique was shown to be a viable technique for removing jammed satellites from the navigation solution depending on the J/S levels. Preplanning the masking elevation angle on the part of the user is required in order to determine acceptable GDOP for the given constellation, location, date and time. More sophisticated techniques to combat RFI are discussed in Appendix G.

During swept CW testing in Tests 9, 10 and 11, the 3D position errors were relatively small compared to the previous CW test results. During Test 9, the maximum

3D position error was 102 meters (excluding one intermittent spike). In Test 10 the maximum 3D position error reached 220 meters, and from Test 11, the maximum 3D error was 122 meters.

During swept CW testing in Test 10, the maximum deviation of the frequency in the tracking channel occurred for the narrowest frequency span tested of 10 kHz, centered on L1 and with a sweep rate of 20 seconds. A J/S level of 30.7 dB from minute 100 to minute 102 and a J/S level of 35.7 dB from minute 110 to 112 resulted in a frequency deviation of up to 20 kHz in some of the tracking channels. The magnitude of deviation was limited by two minute jamming windows and it appears that the deviation would have continued to increase had the jamming been sustained (Figures R.6 and R.8).

The negative bias of approximately 882 Hz in the Doppler frequency offset figures for all tests was attributed to receiver clock drift rate.

In order to generate specific jamming frequency, the signal generator settings were tweaked by measuring the jamming signals during the first two weeks of the pre-test phase. In hindsight, the actual frequencies output by the signal generator had a bias of approximately -280 Hz from the settings on the signal generator. The spectrum analyzer measured the jamming signal within ± 100 Hz of the actual signal seen at the XR5-M receiver.

V. SUMMARY, CONCLUSIONS AND RECOMMENDATIONS

5.1 SUMMARY

The concept of selectively jamming GPS satellites was demonstrated during the course of the thesis research. In particular the generation of a jamming signal using a combination of Doppler shifted jamming signals at a frequency offset and matched with the unique maximum spectral line for each PRN code demonstrated the feasibility of selectively jamming GPS satellites. The spreading of a Continuous Wave (CW) signal into 1000 Hz spectral components within the XR5-M receiver was demonstrated over several tests.

Overall the Hewlett Packard laboratory equipment functioned very well providing the necessary tools to investigate CW and swept CW jamming effects on the commercial-off-the-shelf Navstar XR5-M 12 channel Coarse Acquisition (C/A) code Global Positioning System (GPS) receiver. The linking of two XR5-M receivers provided differentially corrected position information that was used to measure position error as a result of the jamming signals.

At even moderately low Jam to Signal (J/S) values of 20.7 dB, over time, the XR5-M receiver tracking channels were captured by the CW jamming. As J/S levels were increased, the XR5-M receiver tracking channels were captured more quickly by the jamming signals. Of particular interest, the XR5-M receiver tracking channels actually locked on and tracked the CW jamming signals.

A single XR5-M receiver channel locked on to the CW jamming signal, and used in the navigation solution, generated three dimensional (3D) position errors in

excess of 12 kilometers prior to being flagged as an invalid position. Swept CW at high J/S levels of 40.7 dB caused the position output of the XR5-M to freeze but maximum position errors did not exceed 220 meters. Although the swept CW jamming generated much smaller position error than CW jamming, swept CW did result in pulling the tracking channels off frequency by up to 20 kHz.

The ability to access the numerous variables within the XR5-M receiver made it an excellent choice for use in an educational environment. MATLAB[®] 5.2 proved to be a valuable tool for manipulation and analysis of the data output by the XR5-M receiver. A summary of lessons learned during the thesis research is provided in Appendix H and includes such items that did not merit further discussion in this chapter.

5.2 CONCLUSIONS

Based on the results of this thesis research it is concluded that:

- a. Differentially corrected XR5-M 3D position error in the absence of jamming signals had a mean of less than seven meters and displayed periodic multipath interference effects;
- b. CW jamming caused the XR5-M receiver channels to actually gain lock and track the CW signals;
- c. CW jamming generated 3D position errors with a mean of 12.492 kilometers and a maximum 3D position error of 22.999 kilometers prior to the XR5-M receiver flagging the position as invalid;

- d. Swept CW jamming generated a maximum deviation of the tracking channel frequency for the narrowest frequency span investigated of 10 kHz, centered on L1 and with the signal generator set to a sweep time of 20 seconds;
- e. With one exception of an intermittent spike, swept CW interference generated a maximum 3D position error of 220 meters;
- f. The offset of center frequency to match with the maximum spectral lines of a PRN code holds promising results at optimizing jamming for individual satellites;
- g. The equipment used during the research provides the necessary tools to instruct the jamming of GPS signals;
- h. The use of firmware version 3.7 in the XR5-M limited the number of satellites in the navigation solution to only five and differential corrections did not contain RTCM messages Type 20 and 21;
- i. Increasing elevation masking angle improved the performance of the receiver in a jamming environment but also raised the GDOP values increasing position errors during no jamming windows;
- j. The receiver design to use the "carrier lock" of a tracking channel to determine the satellites used in calculating GDOP values can result in a jammed satellite being selected for use in the navigation solution. As a result GPS receiver designers should exercise caution using this technique for receivers which will be used in strong RF interfering environments;

- k. Receiver clock drift rate of approximately 5.6×10^{-7} seconds/second resulted in overall negative shift in all Doppler offset frequencies of approximately 882 Hz;
- l. Maximum Doppler shift of GPS satellites at L1 for a stationary user on the earth's surface at a latitude of 40 degrees is approximately ± 4 kHz;
- m. Data sets and MATLAB[®] code are available for AFIT and CFSAS students to further investigate CW and swept CW jamming effects on a C/A code GPS receiver; and,
- n. The interference effects of wideband noise, replica C/A code and pulsed CW were not investigated.

5.3 RECOMMENDATIONS

The thesis research provided an extremely interesting insight into the effects CW and swept CW jamming on the XR5-M GPS receiver. Based on the results of the twelve tests conducted, it is recommended that:

- a. Further testing be conducted to investigate the potential use of matching CW jamming frequency offset to the maximum spectral lines for each particular PRN code;
- b. Further testing be conducted to investigate swept CW interference with a frequency span between one kHz and 10 kHz and for increased jamming periods;

- c. For future testing the use of a choke ring antenna for the Base Station receiver and an antenna for the Mobile station that is less susceptible to multipath interference be investigated;
- d. Further testing be carried out using wideband noise, pulsed CW, and replica C/A codes as a jamming source;
- e. An upgrade of the XR5-M firmware be investigated;
- f. Increasing elevation angle to minimize jamming effects be used with an understanding of the associated increase in GDOP;
- g. Further testing of other C/A code GPS receivers under similar test conditions be pursued;
- h. For future testing of the XR5-M receiver, periods of more than eight minutes of no jamming be scheduled between actual jamming windows to allow all receiver channels to regain lock;
- i. Designers of C/A code GPS receivers provide a user the ability to set valid fix criteria such as maximum velocity and maximum altitude to minimize position errors as a result of CW interference;
- j. The Canadian Forces (CF) investigate the design and development of GPS jammers into sonobuoys for use in a maritime environment;
- k. Given the magnitude of position error as a result of CW jamming, that the CF conduct testing of in-service GPS receivers to investigate potential vulnerabilities/susceptibility to spoofing by the simple use of CW interference;

- l. The CF incorporate jamming of GPS into all future major exercises involving GPS equipped platforms; and
- m. The CF consider anti-jam capabilities as a high priority for future GPS equipment procurement.

BIBLIOGRAPHY

- [AND98] Anderson, J., and Lucia, D., "GPS Modernization, Advanced Signal Development, Waveform Development Plan," Revision O, 20 March 1998, WWWeb, <http://www.laafb.af.mil/smc/cz/homepage/lm>.
- [BOG97] Boggs, M., and Maraffio, K., "Mitigation Paths for Free Space GPS Jamming," WWWeb, <http://sirius.chinalake.navy.mil/papers.html>.
- [BRAROS98] Braasch, M.S., and Rosen, M.W., "Low-Cost GPS Interference Mitigation Using Single Aperture Cancellation Techniques," 21 January 1998, Institute of Navigation (ION) National Technical Meeting, Long Beach, CA.
- [BRASNY98] Braasch, M.S., and Snyder, C.A., "Running Interference: Testing a Suppression Unit," *GPS World*, Advanstar Communications, Duluth, MN, March 1998.
- [BUT97] Butsch, F., "GPS and GLONASS Radio Interference in Germany," *Proceedings of the Institute of Navigation ION-GPS 1997*, 16-19 September 1997, Kansas City, MO.
- [BUT99] Butcher, S., Navstar Systems Ltd, UK, Personal Correspondence, January 1999.
- [DIV99] Divis, D.A., "Finally A Second Signal," *GPS World*, Advanstar Communications, Duluth, MN, February 1999.
- [DOD97] Office of Assistant Secretary of Defense (Public Affairs), News Release, Reference 095-97. WWWeb, http://www.defenselink.mil/news/Feb97/b022797_bt095-97.html.
- [FAL94] Falen, G.L., "Analysis and Simulation of Narrowband GPS Jamming Using Digital Excision Temporal Filtering," MS Thesis, AFIT/GE/ENG/94D-09, School of Engineering, Air Force Institute of Technology, Wright Patterson AFB OH, December 1994.
- [GWM98] "Gore Announces Safer Skies Agenda," *GPS World*, May 1998, Advanstar Communications, Duluth, MN.
- [HAR93] Harris, G.D., "Analysis and Simulation of A GPS Receiver Design Using Combined Delay-Lock and Modified Tanlock Loops," MS Thesis, AFIT/GE/ENG/93D-13, School of Engineering, Air Force Institute of Technology, Wright Patterson AFB OH, December 1993.
- [HER97] Herskovitz, D., "And the Compass Spun Round and Round, The Coming Era of Navigation Warfare," *Journal of Electronic Defense*, May 1997.

- [HEW67] HP Variable Attenuator Model # 394A, Technical Data Sheet, 15 February 1967.
- [HEW91] *Hewlett Packard HP 8563A Spectrum Analyzer Installation and Verification Manual*, HP Part Number 08563-90042, November 1991.
- [HEW92] HP 8643A Signal Generator, General Information and Specification Sheet, 15 March 1992.
- [ION98] Institute of Navigation, Fall 1998 Newsletter, Alexandria, VA.
- [KAL86] Kalafus, R.M., Van Dierendonck, A.J., Pealer, N.A., "Special Committee 104 Recommendations for Differential GPS Service," *The Institute of Navigation, Volume III*, 1986, Washington, D.C.
- [KAP96] Kaplan, E.D. *Understanding GPS: Principles and Applications*, Boston: Artech House, 1996.
- [LYU97] Lyusin, S.V., Khazanov, I.G., "Techniques for Improving Antijamming Performance of Civil GPS/GLONASS Receivers," *Proceedings of the Institute of Navigation ION-GPS 1997*, 16-19 September 1997, Kansas City, MO.
- [MAE97] Maenpa, J.E., Balodis, M., Walter, G., and Sandholzer, J., "New Interference Rejection Technology from Leica," *Proceedings of the Institute of Navigation ION-GPS 1997*, 16-19 September 1997, Kansas City, MO
- [NAIC96] National Air Intelligence Center Wright-Patterson AFB, OH., "The United States Military Begins to Recognize the Susceptibility of the Global Positioning System to Jamming," 02 February 1996, Report Number NAIC-ID(RS)T-0067-96.
- [NAV93] *Navstar Ltd Power Users Data Monitor Toolkit*, XR5-M 212-PL-G1 issue 1.0, 20 September 1993.
- [NAV96] *Navstar Ltd Control and Display Unit Software Manual*, XR5-M A90-081 Issue 13, 12 August 1996.
- [NAW98] Personal correspondence with NAWC staff at ION 98 GPS Conference, 15-18 September 1998, Nashville, TN.
- [PAR96] Parkinson, B.W., and Spilker, J.J. Jr., *Global Positioning System: Theory and Applications Volume 1 and 2*, (Volume 163 and 164 Progress in Astronautics and Aeronautics), Cambridge: American Institute of Aeronautics and Astronautics, 1996.
- [PET95] Peterson, R.L., Ziemer, R.E., and Borth, D.E., *Introduction to Spread Spectrum Communications*, Upper Saddle River: Prentice Hall, 1995.

[PRI99] Princeton, D., "Loran, Born Again," *Global Airspace*, January 1999, Phillips Business Information, Rockville, MD.

[RAS97] Rash, G., "GPS Jamming in a Laboratory Environment," WWWeb, <http://sirius.chinalake.navy.mil/papers.html>.

[ROU98] Rounds, S.F., "A Low Cost, Unclassified, Direct-Y Code Fast Acquisition Selective Availability Anti-Spoofing Security Module," *Proceedings of the 11th International Technical Meeting of The Satellite Division of the Institute of Navigation ION-GPS 98*, 15-18 September 1998, Nashville, TN.

[SAN97] Sang J., and Kubik, K., "Analysis of Interfered GPS Signals," *Proceedings of the Institute of Navigation ION-GPS 1997*, 16-19 September 1997, Kansas City, MO.

[SEI98] Seife, C., "Where am I?" *New Scientist*, 10 January 1998, WWWeb, <http://www.newscientist.com/ns/980110/ngps.html>.

[UPT98] Upton, D., Upadhyay, T., Marchese, J., and Greskowiak, G., "Commercial-off-the-Shelf (COTS) GPS Interference Canceller and Test Results," *Proceeding of the National Technical Meeting of the Institute of Navigation*, January 1998, Long Beach, CA.

[VAS92] Vasquez, J.R. "Detection of Spoofing, Jamming, or Failure of a Global Positioning System," MS Thesis, AFIT/GE/ENG/92D-37. School of Engineering, Air Force Institute of Technology, Wright Patterson AFB OH, December 1992.

[WAR95] Ward, P.W., "GPS Receiver RF Interference Monitoring, Mitigation, and Analysis Techniques," *Journal of Navigation, ION, Vol.41 No.4*, Winter, 1994-95.

[WAR97] Ward, P.W., "Using a GPS Receiver Monte Carlo Simulator to Predict RF Interference Performance," *Proceedings of the Institute of Navigation ION-GPS 1997*, 16-19 September 1997, Kansas City, MO.

[WAR98] Ward, P.W., "RFI and Jamming Concerns for GNSS and GPS," Navtech Seminars Tutorial, ION GPS-98, Nashville, TN.

[WOL98] Wolfert, R., Chen S., Kohli, S., Leimer, D., and Lascody, J., "Rapid Direct P(Y)-Code Acquisition in a Hostile Environment," *Proceedings of the 11th International Technical Meeting of The Satellite Division of the Institute of Navigation ION-GPS 98*, 15-18 September, 1998, Nashville, TN.

[WWW1] WWWeb, <http://www.acq.osd.mil/at/navwar.htm>, Navigation Warfare Information Regarding Advanced Concept Technology Demonstrations.

[WWW2] WWWeb, http://www.mayflowercom.com/jamming_demonstration_page.htm, "GPS Jamming Effectiveness Table" Mayflower Communications™.

Vita

Major Kenneth D. Johnston was born in Norwood, Ontario, Canada on November 22, 1959. He graduated from Norwood District High School in 1978 and was selected Valedictorian of his graduating class. Following high school he joined the Canadian Forces and attended Royal Roads Military College in Victoria, British Columbia for the first two years of his undergraduate program. He graduated in 1982 with a Bachelor of Science (Applied) degree from the Royal Military College of Kingston, Ontario.

In 1983 he received his Air Navigator wings and was posted to HS 423 Antisubmarine Squadron at Shearwater, Nova Scotia. He served on seagoing Sea King helicopter detachments on HMCS ASSINIBOINE, HMCS ALGONQUIN, and HMCS OTTAWA. While at sea, he participated in several national and NATO exercises. In 1984 he was awarded the Sikorsky Helicopter Rescue Award for saving the life of a member of the crew of the Tall Ship *Marques* which sank in a storm north of Bermuda.

In 1986 he was selected for exchange duties with the Royal Navy with 819 Naval Air Squadron as an Observer on the Mk 5 Sea King, in Prestwick, Scotland. In 1989 he returned to Canada and attended the Canadian Forces School of Aerospace Studies Course. In 1990 he was assigned to the New Shipborne Aircraft Project Management Office in Ottawa, Ontario to pursue the replacement of the aging Sea King with the new EH101 helicopter. In 1993 he was posted to the Helicopter Operational Test and Evaluation Facility (HOTEF) Shearwater, Nova Scotia and served as Project Officer for operational evaluations of acoustic equipment including the AQS-502 Sonar, and underwater locator beacons. Major Johnston was promoted to his present rank in 1996 and remained at HOTEF as the Project Control Officer where he was responsible for all Sea King OT&E projects.

In 1997 he was assigned to the United States Air Force Institute of Technology to earn his Master of Science Degree in Space Operations. Major Johnston is assigned to the Canadian Forces School of Aerospace Studies, Winnipeg, Manitoba following AFIT.