NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

DESIGN, BUILD, AND TEST A HAND-HELD GPS INTERFERENCE DETECTOR

by

John C. Rayburn
James E. Carson

September 2008

Thesis Advisor:	Alex Bordetsky
Second Reader:	Andrew A. Parker

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			*Form Approved OMB No. 0704-0188*
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** September 2008	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE Design, Build, and Test a Hand-held GPS Interference Detector		**5. FUNDING NUMBERS**	
6. AUTHOR(S) MAJ John C. Rayburn (USA) and CPT James E. Carson (USA)			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000		**8. PERFORMING ORGANIZATION REPORT NUMBER**	
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A		**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**	
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited		**12b. DISTRIBUTION CODE** A	

13. ABSTRACT (maximum 200 words)

The Global Positioning System (GPS) navigation signal is extremely vulnerable to intentional and unintentional interference. Increased dependence on GPS by military users has created a need to quickly detect and locate interference at its source. Current methods for detecting and locating GPS interference sources employ a network of multiple sensors to identify interference. The data collected from sensors is then sent to a remote centralized processing station and analyzed to determine the location of the interference source. Although this method has demonstrated effectiveness in this endeavor, it introduces latency between the time of detection at the sensor, and the location of the source. The intent of this thesis is to investigate whether a portable hand held interference detection system can provide more timely detection and location information to provide the actionable intelligence to the disadvantaged GPS users.

14. SUBJECT TERMS GPS, Interference, Jamming, Correlator Output Power, Carrier to Noise Ratio.			**15. NUMBER OF PAGES** 93
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

DESIGN, BUILD, AND TEST A HAND-HELD GPS INTERFERENCE DETECTOR

John C. Rayburn
Major, United States Army
B.S., University of Missouri-Rolla, 1992

James E. Carson
Captain, United States Army
B.S., DeVry University, 2002

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN SPACE SYSTEMS OPERATIONS

from the

NAVAL POSTGRADUATE SCHOOL
September 2008

Author: John C. Rayburn

James E. Carson

Approved by: Alex Bordetsky
Thesis Advisor

Andrew A. Parker
Second Reader

Rudolph Panholzer
Chairman, Space Systems Academic Group

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The Global Positioning System (GPS) navigation signal is extremely vulnerable to intentional and unintentional interference. Increased dependence on GPS by military users has created a need to quickly detect and locate interference at its source. Current methods for detecting and locating GPS interference sources employ a network of multiple sensors to identify interference. The data collected from sensors is then sent to a remote centralized processing station and analyzed to determine the location of the interference source. Although this method has demonstrated effectiveness in this endeavor, it introduces latency between the time of detection at the sensor, and the location of the source. The intent of this thesis is to investigate whether a portable hand held interference detection system can provide more timely detection and location information to provide the actionable intelligence to the disadvantaged GPS users.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

ACKNOWLEDGMENTS

We would first like to thank all the warfighters that we have had the privilege to serve with throughout our careers. It is with the thought of these brave men and women that we have striven, in hopefully some small meaningful way, to improve the body of knowledge that will allow them to remain the greatest fighting force on earth.

At the outset we would like to thank our thesis advisor, Dr. Alex Bordetsky, for his thoughtful understanding and compassion for the many trials and tribulations we have encountered while researching, building, and writing this thesis. His unwavering willingness to provide us with the financial ability to purchase the necessary parts we needed for this thesis is greatly appreciated. Dr. Bordetsky gave us just enough guidance to ensure we continued down the right path, while at the same time allowing us to make numerous mistakes that enabled us to learn new things.

We would also like to state a word of thanks to Professor Andrew A. Parker for willingly accepting taking on the additional duty of being the second reader on our thesis when his plate was already full with other professorial requirements. His technical guidance and direction at the near onset of our research greatly assisted us in wisely using our time by narrowing our focus in the enormous wealth of information surrounding the Global Positioning System.

We would be among the most pitiful people on earth if we failed to thank Mr. Bob Broadston, the NPS Microwave Lab Director. Bob graciously gave us unprecedented access to his lab and equipment to construct our GPS jammer. Most importantly he unselfishly spent numerous hours with us over a month's time assisting us with the complicated and touchy technical aspects behind constructing an Electronic Circuit Board. Bob we cannot fully express our great appreciation and thankfulness for all of your help. Thank You!

We would also like to thank Mr. Robert "Hawg" Haseloff, Senior Operations Analyst of the Joint Navigation Warfare Center for providing us with very useful information almost on a moment's notice.

Finally, we would also like to thank our families for their unending support and understanding during the many hours of research, designing, building, writing, frustration, and stress. We would also like to thank them for being our biggest fans and cheerleaders when we were tempted to succumb to the challenges of our endeavor.

I. INTRODUCTION

Our nation is at war. The United States has been deeply engaged in a war for five plus years against terrorist elements in Iraq, Afghanistan, and various other places around the world. The price being paid in both blood and treasure can never truly be articulated or appreciated. Figure 1 below, which consists of a poignant picture and embedded quote provide the motivation with which this thesis was embarked on.

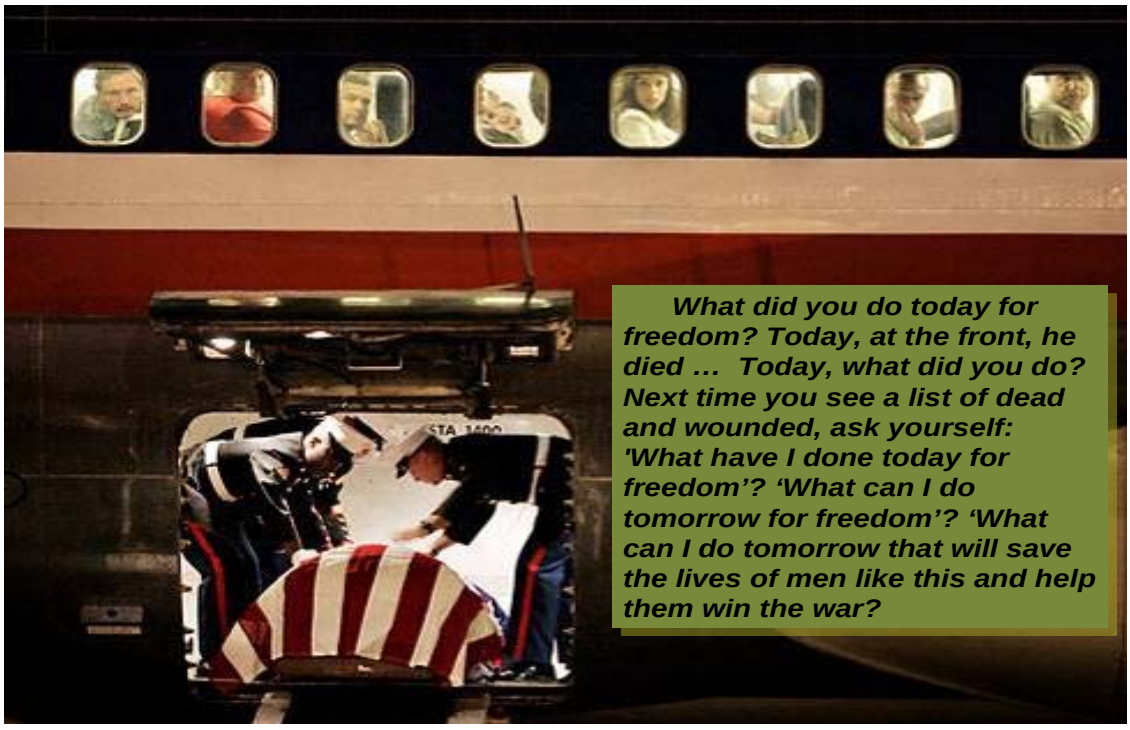

Figure 1. Slide 54 from On Point Warrior-Quotes master copy (From Coffey)[1]

The possible improvement in increased combat lethality and survivability that may be obtained by the work included in this thesis is wholly dedicated as a small means of addressing the question in the figure above: "What can I do tomorrow that will save the lives of men like this and help them win the war?"

1 Bill Coffey, U.S. Army Space and Missile Defense Command (SMDC), On Point Warrior Quotes-Master Copy (Slide 54 of Powerpoint Presentation), 2008 Mass E-Mail (accessed July 13, 2008).

The Global Positioning System (GPS), a highly reliable Position, Navigation, and Timing (PNT) system, has become a ubiquitous capability for both civil and military applications. The civil capabilities provided by GPS are now so thoroughly embedded in the day-to-day lives of people throughout the world that any interruption in this service would cause tremendous problems in numerous areas. GPS provides the information necessary for commercial aircraft take-off and landing abilities, end-to-end logistics monitoring for businesses supply chain management, personal and business navigation, and highly accurate surveying, to name a few. Figure 2 illustrates several of the technologies systems and operations functions that are reliant upon GPS.

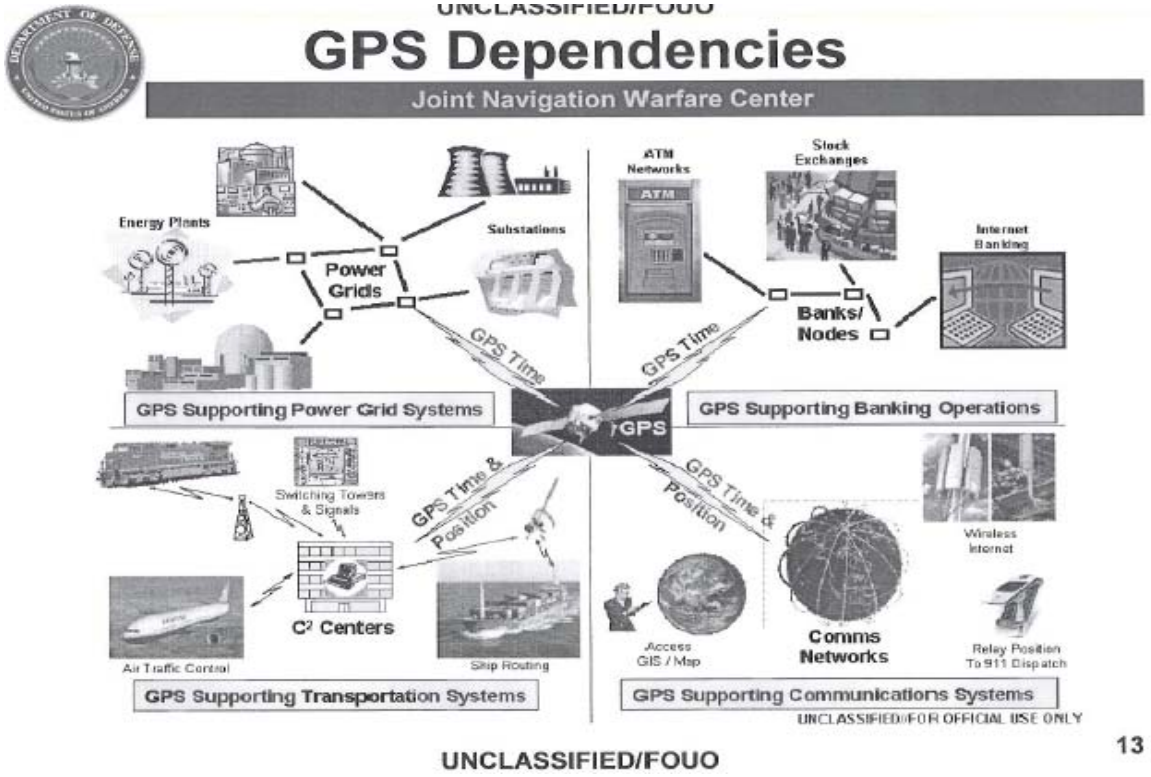

Figure 2. GPS Dependent Systems and Operations (After JNWC-Navwar-Threat Overview Brief)[2]

2 Robert "Hawg" Haseloff, "JNWC-Navwar-Threat Overview Brief (Unclassified Portion) United States Army FA-40 Symposium" (Colorado Springs, Colorado, Joint Navigation Warfare Center, 2-5 September 2008) (accessed 12 September 2008).

The effects obtained by denial of this GPS service to U.S. military applications also creates the potential to cause devastating consequences by eliminating or degrading U.S. superiority in a myriad of military systems which use the information provided by GPS. There are several different types of jammers and sources of interference which have the ability to deny, degrade, and/or disrupt the GPS signal from coherently providing its sought after information. Figure 3 lists several of the jamming methods, as well as, Electro-Magnetic Interference.

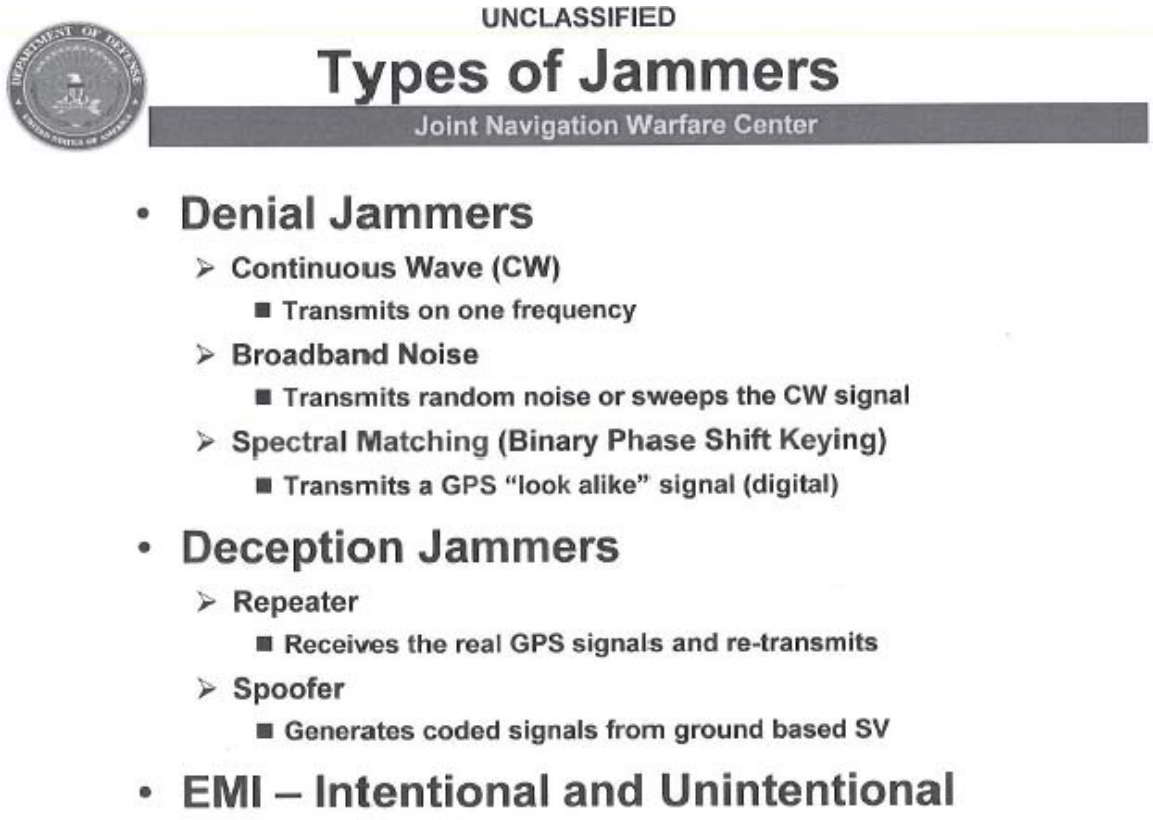

Figure 3. Types of Jammers and Interference which affect the GPS Signal (From JNWC-Navwar-Threat Overview Brief)[3]

3 Robert "Hawg" Haseloff, "JNWC-Navwar-Threat Overview Brief (Unclassified Portion) United States Army FA-40 Symposium" (Colorado Springs, Colorado, Joint Navigation Warfare Center, 2-5 September 2008) (accessed 12 September 2008).

The enemies of the United States are acutely aware of this potential Achilles heel and are actively seeking ways to exploit this potential weakness. One of the major ways that they are trying to achieve this is through effective jamming of GPS signals

> At the Paris Air Show in 1999, a Russian company called Aviaconversia demonstrated a 4-watt GPS jammer. The jammer weighed about 19 pounds and was capable of denying GPS reception for more than 100 miles. Many such jammers are available through the Internet for as little as $39.9 [$3999].[4]

The previous quote taken from an anonymous source on the Internet clearly demonstrates that there is both a demand and an industry out there capable of providing low-cost GPS jammers that are effective over fairly long ranges. Figure 4 shows an Aviaconversia 4W GPS Jammer that was offered for sale at the Moscow Air show in 1997. Knowing that these types of inexpensive GPS jammers are readily available, in addition to their more powerful military-grade counterparts, it becomes blatantly obvious that our military forces must have a rapid and effective means of identifying these jamming sources so that their interfering signals may be neutralized.

4 Wikipedia contributors, "Aviaconversiya," Wikipedia, The Free Encyclopedia, http://it.wikipedia.org/wiki/aviaconversiya?oldid=17841971 (accessed 19 September 2008).

Figure 4. Aviaconversia 4W GPS Jammer[5]

As previously stated, relatively low power GPS jammers are effective over extensive ranges, especially if they are employed from the air in which they have a straight line of sight signal path which is less impeded by obstacles on the ground. Figure 5 illustrates jammers at various power levels and their effective ranges when compared to the power levels required to affect various levels of GPS Acquisition. Figure 6 gives a graphical representation of the effectiveness of a four-watt jammer employed from both the ground and the air. Figure 6 also illustrates the significant differences of effective GPS jamming ranges when comparing land-based jamming which has many obstacles such as terrain, vegetation, buildings, etcetera to block or attenuate the jamming signal and that jamming which occurs in the air and unimpeded by

5 Rockwell International, "GPS Jamming," Rockwell International, http://www.ac11.org/gps1.htm, (accessed 10 September 2008).

anything except the natural physical characteristics of the airspace. Figure 6 further shows that loss of lock due to air-based jamming occurs at 38km and for land-based jamming loss of lock doesn't occur until you get within 1km.

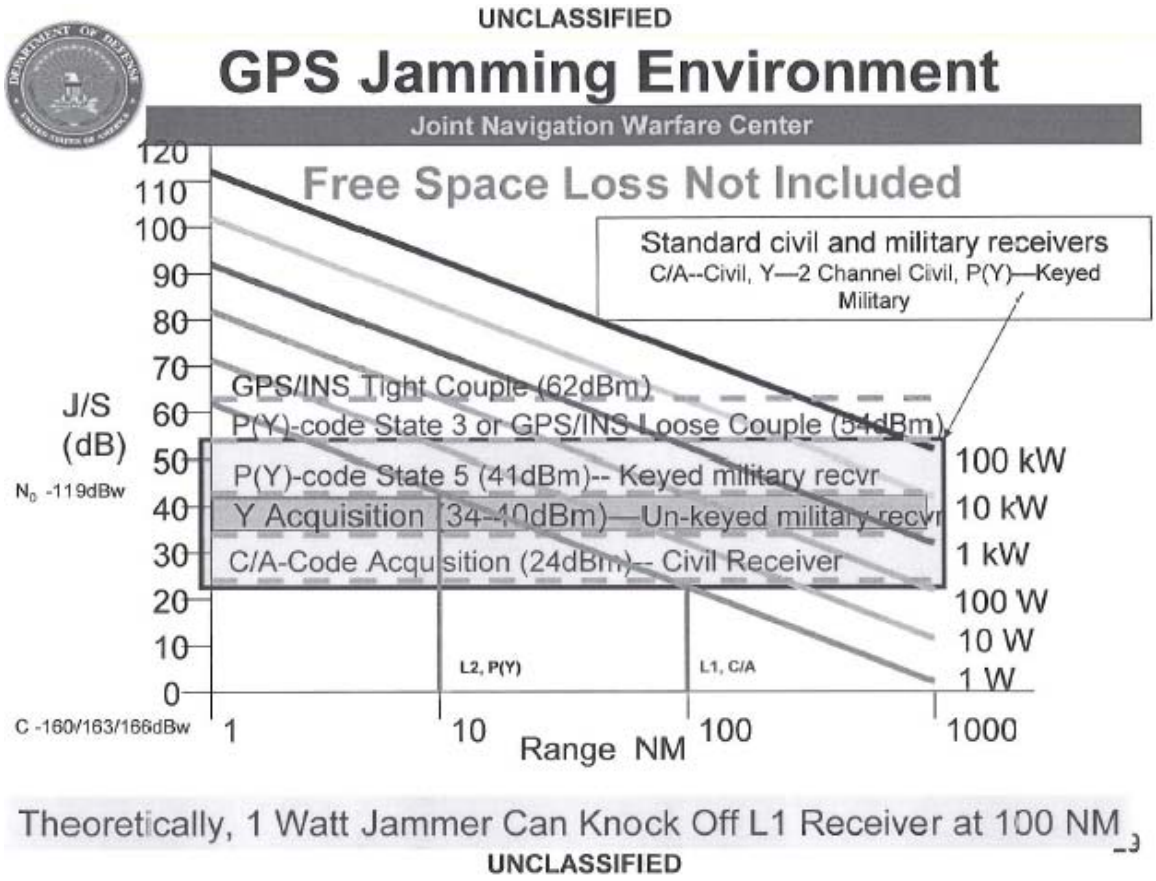

Figure 5. Jammer effects versus distance (From JNWC-Navwar-Threat Overview Brief)[6]

6 Haseloff, JNWC-Navwar-Threat Overview Brief (Unclassified Portion) United States Army FA-40 Symposium, 1-2-30

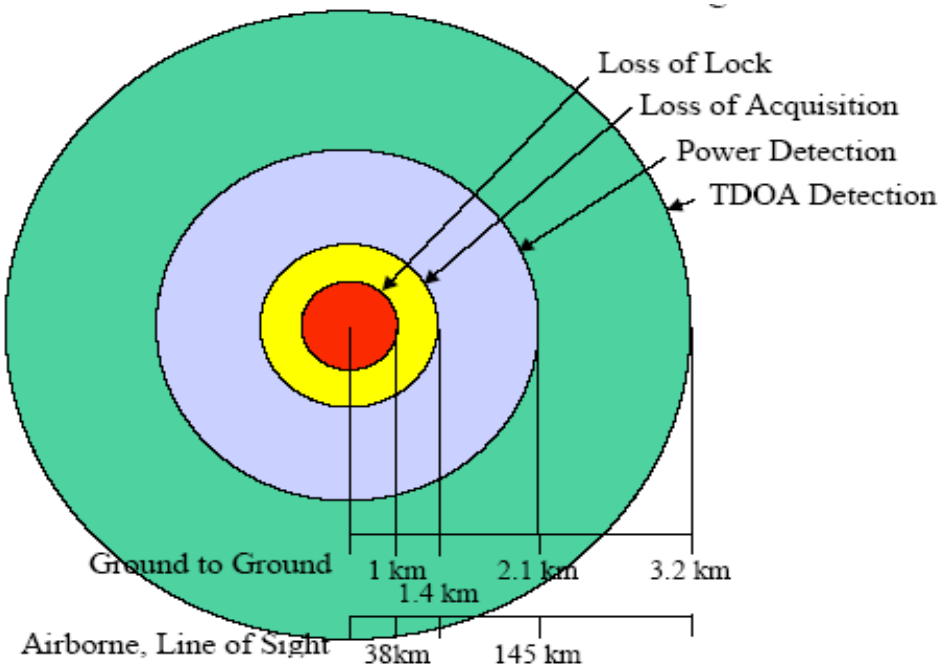

Figure 6. Received Jammer/Signal (J/S) as a Function of Distance from Jammer (From Brown, Reynolds, Roberts, and Serie)[7]

Since the onset of declared Full Operational Capability of the GPS satellite constellation on April 27, 1995[8] by Air Force Space Command, GPS satellites have become an essential element in the United States military's arsenal to fight in and win this nation's wars. GPS satellites provide the PNT information necessary for our forces to have and maintain the situational awareness to know when and where they're at while stationary or on the move. The kind of information provided by GPS is essential regardless of if you're using it for force tracking and situational awareness as in Blue Force Tracking (BFT)/Blue Force Situational Awareness (BFSA), using it to provide highly accurate position and navigation information to direct smart munitions, or using it to assist in the conduct of Combat Search and Rescue (CSAR) missions.

7 Alison Brown and others, "Jammer and Interference Location System - Design and Initial Test" Alexandria, 1999).

8 United States Naval Observatory, "USNO NAVSTAR Global Positioning System," http://tycho.usno.navy.mil/gpsinfo.html (accessed 19 September 2008).

The challenge of monitoring GPS signals for interference (intentional or unintentional) and analyzing the effects that this interference has on current and future operations are issues that are being brought up by those space warriors recently returning from deployments in Iraq and Afghanistan.

> *Position, Navigation, and Timing* Navigation through the use of satellites allows for extremely accurate maneuver and targeting. Many systems also depend on Global Positioning System (GPS) timing for the synchronization of communications. The number of land force systems that have an integrated GPS receiver is large and growing, to the point that numerous missions are dependent on it. Widespread use of GPS in military operations in the last few years has uncovered unforeseen problems, and Army and Marine unit staffs are now routinely required to resolve complex, technical anomalies with GPS in support of operations. Furthermore, staff members must monitor the accuracy of GPS and the effect this accuracy may have on current and planned operations.[9]

It is with these challenges in mind that this thesis seeks to address the issue of GPS Jamming and/or interference by attempting to identify its source and location. The idea of GPS jamming and interference location detection is nothing new; it has been going on for almost as long as GPS has been in existence.

There are several programs both unclassified and classified that address the challenge of GPS jamming. A Jammer Location (JLOC)[10] System approach is a system that has been suggested to use numerous receivers that send back their GPS information to a centralized processing station, which calibrates their information against a known grid coordinate that has previously been taken prior to the onset of jamming. This known coordinate is then compared to a receiver reported coordinate during jamming and the difference is obtained. This is done for several known locations in a given area of operations. These known deviations are then calibrated for the various other receivers throughout the area of operations. Knowing these deviations, analysis can then be done

9 Bob Guerriero, LTC, Tom James, LTC and Jim Rozzi, LTC, "The Future of Army Space Forces - A Vision to Optimize Tactical and Operational Space Support," The Army Space Journal, 2007, 12, http://www.smdc-armyforces.army.mil/ASJ/Edition.asp?E=2 (accessed 13 July 2008).

10 Brown and others, Jammer and Interference Location System - Design and Initial Test

to ascertain the most likely source and location of the jammer. This system would provide for a centralized analysis and processing hub that could be queried to try to determine jamming and interference that has already occurred.

The problem to date, at least from a forward-deployed soldier perspective, is that although a jammer location may be able to eventually be determined, the time it takes is not responsive enough to allow for these soldiers to continue the mission unimpeded. The main objective of this thesis is to make inroads towards coming up with an initial design of a hand-held GPS interference detector that could provide actionable intelligence to forward-deployed, disadvantaged soldiers which allows them to take the immediate, necessary action to terminate that interference.

THIS PAGE INTENTIONALLY LEFT BLANK

II. GPS LINK BUDGET

The amount of power available to terrestrial GPS receivers is extremely low. Figure 7 provides some practical perspective to illustrate just how modest this power level is and why the GPS signal is susceptible to jamming over great distances with a low power jammer.

Figure 7. Signal Strength comparisons with the GPS Signal (From JNWC-Navwar-Threat Overview Brief)[11]

A. THE GENERAL LINK BUDGET EQUATION

In order to establish a successful communications link, orbiting GPS satellites and terrestrial-based GPS receivers must meet the requirements of the link budget equation. The general link budget equation is given by: $S_R = P_t + L_l + G_t + L_{fs} + G_r + L_o$, where,

- S_R = Received signal power

11 Haseloff, JNWC-Navwar-Threat Overview Brief (Unclassified Portion) United States Army FA-40 Symposium, 1-2-30

- P_t = Satellite transmitter power
- L_l = Transmitter line losses
- G_t = Satellite transmitter antenna gain
- L_{fs} = Loss due to free space
- G_r = Receiver antenna gain
- L_o = Other losses

Each of the terms in the link budget equation represented as either power or gain is assigned a positive value, while those annotated as losses are assigned a negative value. The sum of all the gains and losses determines the power available at the GPS receiver. The minimum power requirement at the receiver is based on a quantity known as the signal-to-noise ratio or SNR. Figure 8 depicts both the Jammer-to-Signal Ratio (JSR) and SNR for a given set of testing.

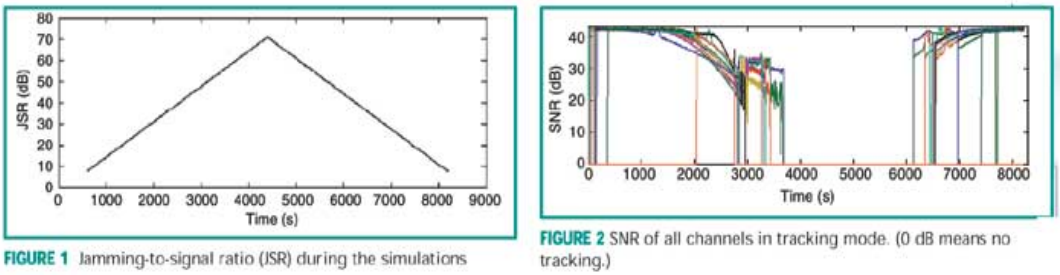

Figure 8. Jammer-to-Signal Ratio and SNR graphs (From GPS World)[12]

As its name suggests, the SNR is formed by the ratio of the received signal power, S_R to the noise power. Noise power, N, is given by: $N = kTB$, where,

- k = the Boltzmann's constant 1.38×10^{-23} Joules/K
- T = the receiver temperature in degrees Kelvin
- B = Bandwidth of the receiver in Hertz

As a general rule of thumb, the minimum power required to establish a link is determined by a receiver signal power that is 10 decibels above the noise power.

12 Borje Forssell and Trond Olsen, "GPS World - Jamming GPS," GPS World, http://www.gpsworld.com/gpsworld/content/printContentPopup.jsp?id=43432 (accessed 19 September 2008).

The sum formed by the first three terms in the link equation is often referred to as the Effective Isotropic Radiated Power, or EIRP. This combined term is generally used to calculate a link budget when the individual terms are not available. Each GPS satellite is equipped with multiple transmitters for which the EIRP is known. The transmitters are dedicated to emitting at 1575.42 MHz and 1227.60 MHz. Each of these frequencies is commonly referred to as the L1 and L2 link respectively

1. L1 Link

The L1 link has the following terms in the link equation:

- EIRP = $P_t + L_l + G_t$ = 26.8 dBW
- L_{fs} = -184.4 dBW
- G_r = 3 dBW
- L_o = -5.4 dBW

This gives the power available to the receiver as:

- $S_R = EIRP + L_{fs} + G_r + L_o$ = -160 dBW or $1x10^{-16}$ W[13]

All GPS receivers must have the sensitivity to detect this extremely low power signal to establish a link.

2. L2 Link

The L2 link has the following terms in the link equation:

- EIRP = $P_t + L_l + G_t$ = 19.7 dBW
- L_{fs} = -182.3 dBW
- G_r = 3 dBW
- L_o = -6.4 dBW

This gives the power available to the receiver as:

- $S_R = EIRP + L_{fs} + G_r + L_o$ = -166 dBW or $2.5x10^{-17}$ W[14]

---

13 Navtech GPS, "GPS L1 Link Budget," http://www.navtechgps.com/pdf/GPS L1 Link Budget ERP.pdf (accessed 22 September 2008).

14 Navtech GPS, "GPS L2 Link Budget," http://www.navtechgps.com/pdf/GpsNetworking_LinkBudget.pdf (accessed 22 September 2008).

As demonstrated in Figure 9, the receiver power quantities for both the L1 and L2 links at are at relatively low levels. GPS receivers sensitive enough to detect these low power levels are also susceptible to local interference from transmitters operating on the same frequency.

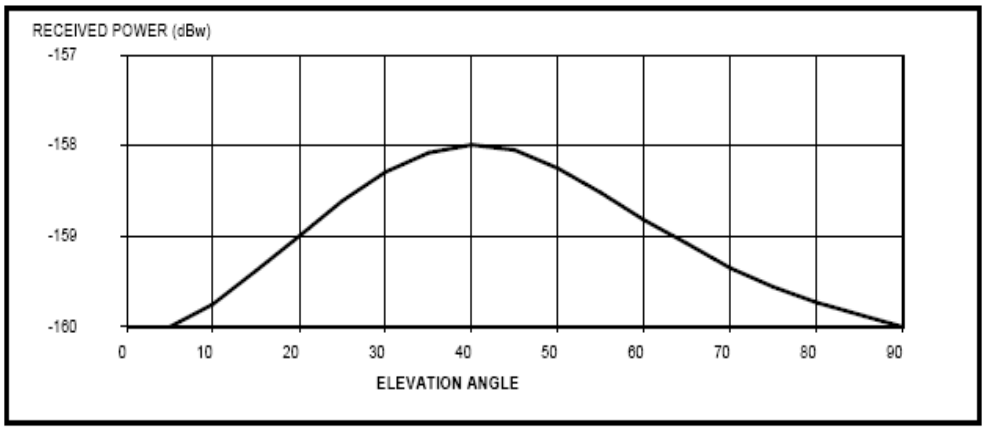

Figure 9. GPS Signal Strength Level vs. Elevation Angle (From Global Positioning System Standard Positioning Service Signal Specification)[15]

15 USCG, "Global Positioning System Standard Positioning Service Signal Specification, 2nd Edition," USCG, http://www.navcen.uscg.gov/pubs/gps/sigspec/gpssps1.pdf (accessed 14 August 2008).

III. METHODS OF DETECTION AND LOCALIZATION

There are numerous methods available for detecting interference on GPS signals. When one considers that the GPS signals (L1 and L2) are nothing more than RF signals at their respective frequencies it becomes amazingly clear just how susceptible they are to interference, whether it be intentional or not. Knowing the reliability or certainty of the information given by a system is of utmost importance to the user. The trustworthiness of the information obtained has also been described as the integrity of the system.

> Integrity can be defined as a measure of confidence on the specified accuracy of any given system. Precision GPS applications such CAT II/III aircraft landings place demands for high levels of integrity from a GPS receiver, given the risks involved. Unfortunately RF interference, which occurs frequently in the operating environment of a GPS receiver, can surreptitiously degrade accuracy, and thereby compromise the integrity of the receiver. Such interference may be intentional (from an RF jammer) or non-intentional, as would result from channel cohabitance or harmonics from mobile cellular, satellite, TV and FM radio.[16]

Analyzing the integrity of the GPS signal at the receiver location allows for the determination of whether the signal is experiencing interference or not. One of the most pressing problems that is not addressed by receivers themselves is the challenge of noise and how that may affect the pseudorange error of a GPS signal. The higher the noise from either a Continuous Wave (CW) source or an Additive White Gaussian Noise (AWGN) source on a GPS RF signal causes the Carrier-to-Noise (C/No) ratio to be reduced which in turn causes the pseudorange error to increase. This detrimental error to the GPS accuracy could go totally unnoticed if there were not some sort of analysis being automatically done on the signal to ensure that this type of induced error was not occurring. Some of the more common and familiar methods of testing the integrity of an RF signal in use these days are: Correlator Output Power, Variance of Correlator Output

16 Awele Ndili, Stanford University and Dr. Per Enge, Stanford University, "GPS Receiver Autonomous Interference Detection" (http://waas.stanford.edu/~wwu/papers/gps/PDF/interfere_detect_ann98.pdf, April 1998) (accessed 30 July 2008).

Power, Carrier Phase Vacillation, Active Gain Control (AGC) Control Loop Gain, Multiple-Model Adaptive Estimation (MMAE), and Receiver Estimation of C/No.

After determining that interference is occurring on the GPS Signal, it is then useful to know where that interference is emanating from so that actions can be taken to resolve the interference problem. The challenge of localization of the interference is one that can be approached from numerous directions as well. Three of the most common approaches to localization of RF interference are by using the following: Carrier/Noise Jammer Location Sensor, Angle of Arrival Jammer Location Sensor, and Time Difference of Arrival Jammer Location Sensor. Let's first take a look at the interference detection methods.

A. DETECTION

1. Correlator Output Power (COP)

Correlator Output Power as defined by Awele Ndili and Dr. Per Enge of Stanford University at their presentation at the 1998 IEEE Position, Location and Navigation Symposium – PLANS '98 is:

> The correlator output power (COP) is a quantity computed in the receiver which gives an indication of the average post-correlation signal to noise ratio. It is computed from equation 1 below:
>
> $$Correlator\ Output\ Power = I^2 + Q^2 / Expected\ Noise\ Floor \qquad (1)$$
>
> where I and Q are the 1ms-averaged in-phase and quadrature prompt correlator signal. Expected noise floor is receiver specific, and is derived from statistic expectations for a specific receiver digital implementation.[17]

17 Awele Ndili, Stanford University and Dr. Per Enge, Stanford University, "GPS Receiver Autonomous Interference Detection" (http://waas.stanford.edu/~wwu/papers/gps/PDF/interfere_detect_ann98.pdf, April 1998) (accessed 30 July 2008).

Looking at the equation given in the quote above it becomes readily apparent that for a specific receiver with a known expected noise floor and the measurements of the in-phase and quadrature signals, the characteristic COP can be calculated for a given receiver. A different value for COP indicates that some type of noise interference may be occurring due to a decrease in COP.

2. Variance of Correlator Output Power

Correlator Output Power variance is exactly as the name implies, it is the variance of the Correlator Output Power. Variance is the standard mathematical and statistical definition of variance, which is the square of the standard deviation. The idea of using COP variances as a metric for the integrity of a GPS signal are due to the fact that they serve as robust indices, in various types of jamming environments, to illustrate changes to GPS signals as encountered at the receiver. In Figure 10 below, Ndili and Enge graphically depict the effects that interference has on COP variance beginning with interference and through reacquisition of the GPS signal. Figure 10 clearly illustrates the decrease in variance between the signal being subjected to interference and then not, from roughly 25dB to approximately 6 or 7dB. It is also easily observable the step increase in the COP when cycling out of interference.

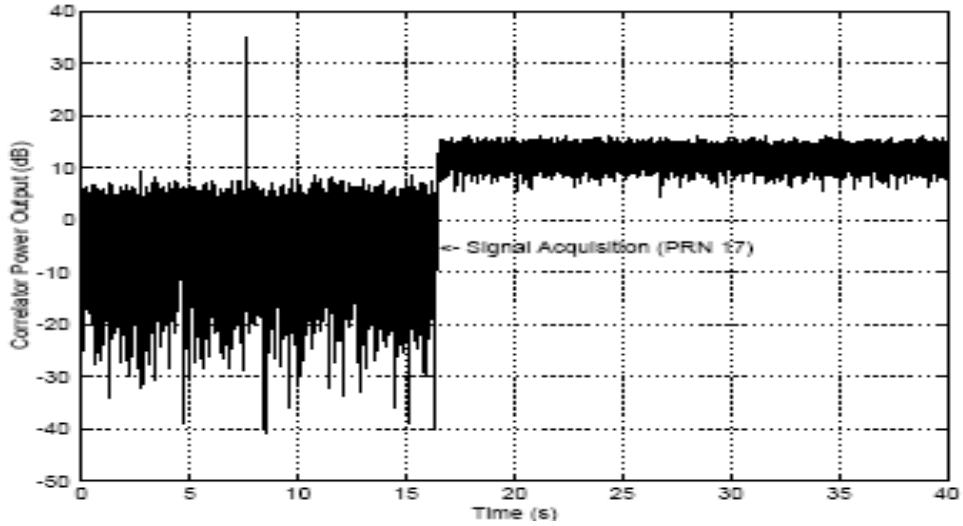

Figure 10. Correlator Output Power for a GPS Receiver (From Ndili & Enge)[18]

3. Carrier Phase Vacillation

This metric examines the fluctuation of carrier phasor angles of the GPS signal with respect to time. It has been shown that these variances in the phasor angles are a function of the level of noise within the signal. Articulated in a more precise manner:

> Carrier phase vacillation provides a measure of the variance or jitter in carrier phase measurements from one measurement epoch to the next, and is defined here as:
>
> *Carrier Phase Vacillation* =
>
> $$Time\ average[abs\{Carrier\ Phase_i - Carrier\ Phase_{i-1}\}]$$
>
> where i is the 1 ms epoch index.[19]

18 Awele Ndili, Stanford University and Dr. Per Enge, Stanford University, "GPS Receiver Autonomous Interference Detection" (http://waas.stanford.edu/~wwu/papers/gps/PDF/interfere_detect_ann98.pdf, April 1998) (accessed 30 July 2008).

19 Awele Ndili, Stanford University and Dr. Per Enge, Stanford University, "GPS Receiver Autonomous Interference Detection" (http://waas.stanford.edu/~wwu/papers/gps/PDF/interfere_detect_ann98.pdf, April 1998) (accessed 30 July 2008).

This carrier phase vacillation is a robust indicator of the level of noise present in a signal and is therefore also a good choice for using as an identifier of interference. Noise comes not only from that generated by the interference signal, but also that noise that is inherent within the receiver clock. Figure 11 provides a graphic example of the effects of noise on the carrier phasor angles of a GPS signal.

The data used to generate this graph comes from the arctangent of the in-phase and quadrature signal phase measurements. For this particular plot, the carrier phase vacillation is approximately 11 degrees.

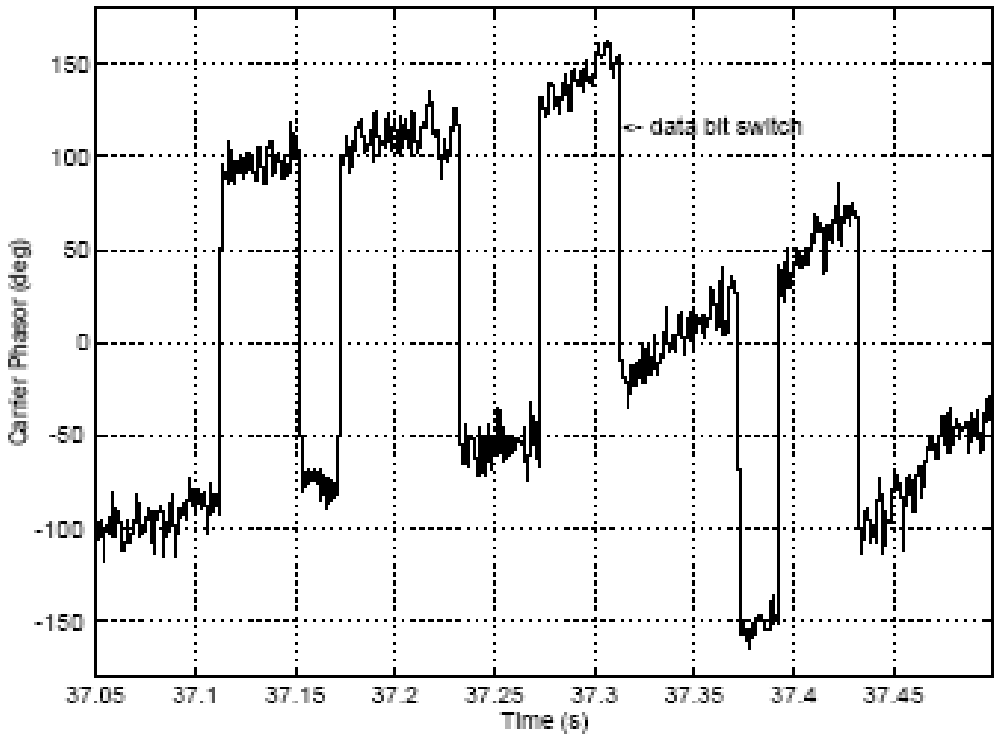

Figure 11. Carrier Phase for a GPS Receiver with a FLL Carrier Tracking Loop (From Ndili & Enge)[20]

20 Awele Ndili, Stanford University and Dr. Per Enge, Stanford University, "GPS Receiver Autonomous Interference Detection" (http://waas.stanford.edu/~wwu/papers/gps/PDF/interfere_detect_ann98.pdf, April 1998) (accessed 30 July 2008).

4. Active Gain Control (AGC) Control Loop Gain

Active Gain Control is another test statistic that is useful in identifying and corroborating that interference, in the form of pseudorange error, is occurring on a signal. The analog signal from GPS is digitized and converted to a digital signal by means of a converter that is set to maintain a specified ratio of digitized signal output levels. The linear relationship between increase AGC and increased pseudorange error generally holds, except in the cases of satellite signal attenuation and pulsed CW and pulsed AWGN interference. See Figure 12 which provides the data plots of an experiment illustrating these attributes and relationships.

In the case of signal attenuation, this result is expected. AGC is impacted by the total power of incoming signals from all satellites in view and therefore the depletion of one satellite's signal power will not have as significant an impact on AGC gain as one might think. Therefore, in the case of spacecraft vehicle signal attenuation, AGC Control Loop Gain is not a metric for determining interference.

For the scenario of pulsed CW and pulsed AWGN interference it has been shown that a linear relationship between these pulsed interferences' pseudorange error and AGC gain does not exist either. Early on, the pseudorange error generally becomes unaffected by increases in AGC, therefore no one-to-one linear relationship. Here again, in the cases of pulsed CW and pulsed AWGN, AGC Control Loop Gain would not be a wise selection as the sole determination of interference occurring for a given signal.

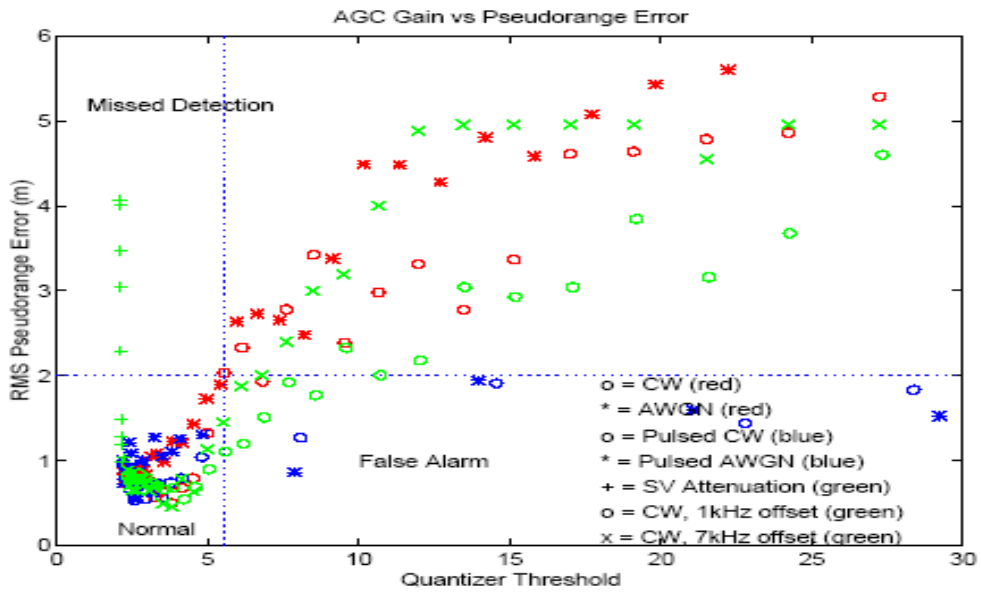

Figure 12. Pseudorange Error vs. AGC Gain (From Ndili and Eng)[21]

One thing noted in the paper by Ndili and Enge,

> This peculiarity of AGC gain can be used in conjunction with other test statistics to discriminate between pseudorange accuracy degradation due to pulsed and non-pulsed interference, and signal blockage.[22]

For example, if one referred to the COP, COP variance, Carrier Phase Vacillation metrics they could determine that interference was occurring. If they also looked at the AGC Gain and noted no significant increase in pseudorange error this would indicate that some type of pulsed jamming (CW or AWGN) was occurring.

---

21 Awele Ndili, Stanford University and Dr. Per Enge, Stanford University, "GPS Receiver Autonomous Interference Detection" (http://waas.stanford.edu/~wwu/papers/gps/PDF/interfere_detect_ann98.pdf, April 1998) (accessed 30 July 2008).

22 Awele Ndili, Stanford University and Dr. Per Enge, Stanford University, "GPS Receiver Autonomous Interference Detection" (http://waas.stanford.edu/~wwu/papers/gps/PDF/interfere_detect_ann98.pdf, April 1998) (accessed 30 July 2008).

On the other hand, if they noted from the AGC Gain versus Pseudorange error plot that pseudorange error was increasing without any significant increase in the quantizer threshold, this would indicate that Spacecraft Vehicle attenuation might be the culprit for the interference.

5. Multiple-Model Adaptive Estimation (MMAE)

Multiple-Model Adaptive Estimation (MMAE) is another method used to detect interference on a GPS signal. MMAE makes use of the estimation prowess of Kalman filters in order to provide a best guess for accurate information. In an October 1998 paper in IEEE by White, Maybeck, and DeVilbiss they described the MMAE process as follows:

> Such an MMAE is composed of a bank of parallel filters, each hypothesizing a different failure status, along with an evaluation of the current probability of each hypothesis being correct, to form a probability-weighted average state estimate as an output.
>
> For interference/jamming degradation represented as increased measurement noise variance, simulation results show that, because of the good failure detection and isolation (FDI) performance using MMAE, the blended navigation performance is essentially that of a single extended Kalman filter (EKF) artificially informed of the actual interference noise variance.[23]

Basically, the MMAE process consists of taking the information obtained from a sensor and passing that information through various Kalman filters that have been set up to model various environments and conditions that might be experienced by the sensor. This information is then sent out from the Kalman filters in the form of a computed state vector and its corresponding residuals. The size of residuals obtained is an indicator as to the level of agreement between that particular Kalman filter's model and that actual information obtained from the sensor. The residual information is analyzed by a Conditional Probability Weighting Computation which determines the probability of

23 Nathan A. White, Peter S. Maybeck and Stewart DeVilbiss, "Detection of interference/jamming and Spoofing in a DGPS-Aided Inertial System," IEEE Transactions on Aerospace and Electronic Systems 34, no. 4 (IEEE Transactions on Aerospace and Electronic Systems. Vol. 34, no. 4, pp. 1208-1217. October 1998), 1208-1217.

model accuracy for this Kalman filter. This is done for every Kalman filter and then the individual probabilities are then reconstituted back together and a Bayesian blended estimate is then given. Figure 13 pictorially depicts the MMAE process.

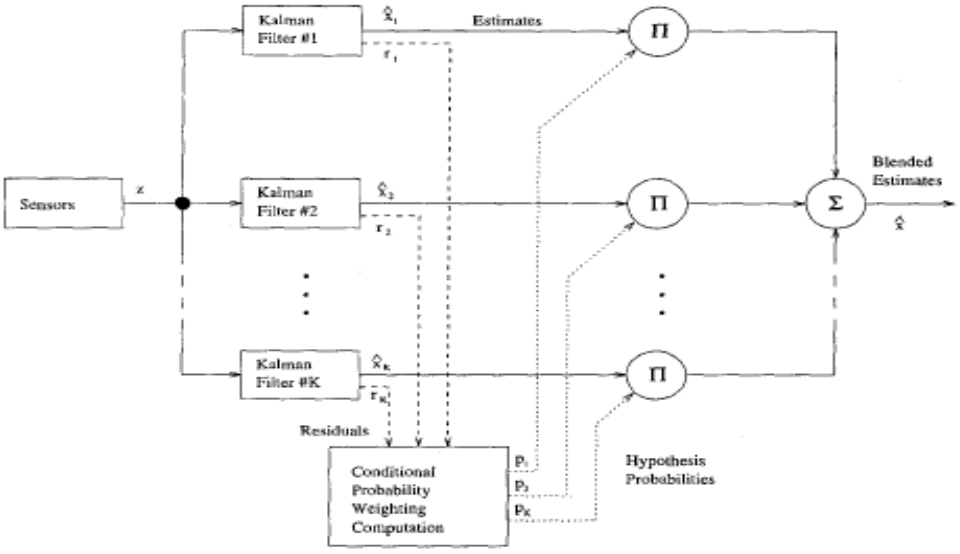

Figure 13. MMAE Estimation process (From White, Maybeck, & DeVilbiss)[24]

6. Receiver Estimation of C/No

This approach at the detection and characterization of CW interference is one of the more recent attempts and was presented in April 2006 at the Position, Location, and Navigation Symposium for IEEE/ION. The title of the paper is: "A Novel Approach in Detection and Characterization of CW Interference of GPS Signal Using Receiver Estimation of C/No." This approach uses some of the previously described metrics and then seeks to slim down the hardware and software requirements necessary to do this.

> In this paper, AGC level together with correlator output power is used to detect and characterize the RFI but the difference is that the receiver simply uses a standard correlator. The other advantage of this algorithm is

24 Awele Ndili, Stanford University and Dr. Per Enge, Stanford University, "GPS Receiver Autonomous Interference Detection" (http://waas.stanford.edu/~wwu/papers/gps/PDF/interfere_detect_ann98.pdf, April 1998) , (accessed 30 July 2008).

> that it is capable of detecting and characterizing CW RFI even if it is not close in frequency to any of the C/A code spectral lines.[25]

The overall thrust of this method of detection and characterization is to compare the theoretical C/No with the actual C/No and then using this information along with the knowledge of the structure of the GPS C/A code, then the existence and characterization of the interference can be determined.

Figure 14 illustrates the process by which the C/A code is combined with the navigation data and then the CW RFI and noise are added. It is then shown that the incoming code is compared and multiplied by the receiver's replica code and then the tracking loop's low pass filter filters out data and interference outside the bandwidth. The take away behind the set of graphs within this consolidated figure is to illustrate that J_before (interference power before) is different than J_after (interference power after). The value of J_after is determined by the strength of the nearest line to the interference. The following quote describes why this is important.

> Now, if we have an RFI with fixed frequency and a GPS signal with Doppler frequency that varies with satellite motion, over time the RFI coincides with several different consecutive lines in the spectrum. Each of these lines has its own unique effect on the remaining interference in the output of the loops. We propose to examine the effect of a series of lines, and thus calculate the frequency of the RFI. The quantity that can best reflect this effect is the correlator output power. Carrier to noise ratio which quantifies the quality of the signal is the parameter which is use for this purpose.[26]

Figure 15 graphically depicts the correlator process at the receiver. This figure illustrates the fact that the incoming GPS signal gets processed through both a code tracking loop as well as a carrier tracking loop, which consists of both the In-Phase and

25 A.T. Balaei, A. G. Dempster, and J. Barnes, A Novel Approach in Detection and Characterization of CW Interference of GPS Signal using Receiver Estimation of C/No, 2006), 1120-1126.

26 A. T. Balaei, A. G. Dempster, and J. Barnes, A Novel Approach in Detection and Characterization of CW Interference of GPS Signal using Receiver Estimation of C/No, 2006), 1120-1126.

Quadrature portions of the signal being passed through low-pass filters and combined and then fed back through a low-pass filter and oscillator and then back to be combined with the C/A code.

Figure 1 Spreading the data over the C/A code spectrum bandwidth

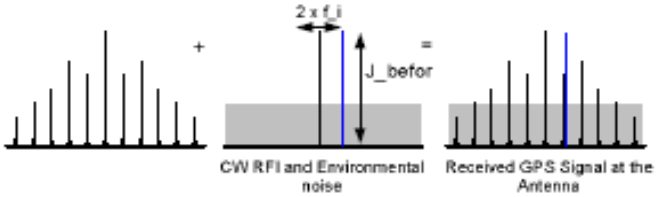

Figure 2 Interference and background noise is added to make the final GPS signal received at the antenna

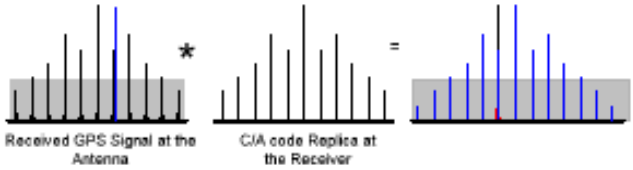

Figure 3 Code is despread by getting multiplied by the receiver code replica and interference is spread

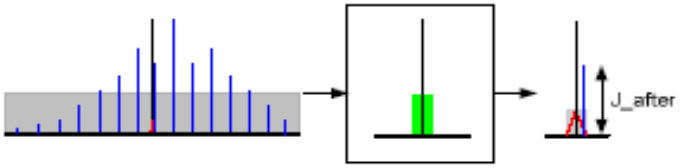

Figure 4 Tracking loop low pass filter, filters the data and the interference which is outside the filter bandwidth out

Figure 14. Development of C/A code with CW RFI then passed through a receiver's low pass filter (After Balaei, Dempster, and Barnes)[27]

27 A. T. Balaei, A. G. Dempster and J. Barnes, A Novel Approach in Detection and Characterization of CW Interference of GPS Signal using Receiver Estimation of C/No, 2006), 1120-1126.

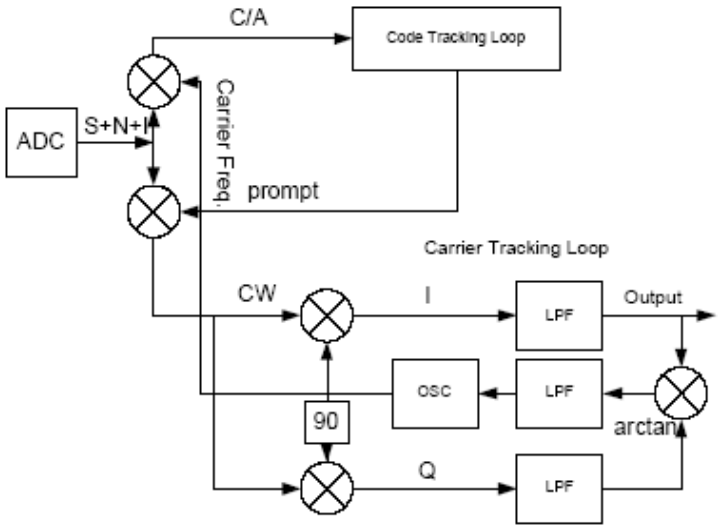

Figure 15. Correlator (Code and Carrier Tracking Loops) (From Balaei, Dempster, and Barnes)[28]

The expression for the *theoretical* C/No was also previously developed by the same authors who authored the above approach. In their previous work they developed the equation for C/No to be as follows:

$$\mathrm{C/No} = \frac{(\mathrm{T_d} R_0(\tau).\mathrm{sinc}(\Delta f_c T_d))^2}{L_n N_0 + (\mathrm{Td.C_n.sinc(Td.\Delta f_i)})^2} \quad 29$$

This was then slightly altered in their more recent work to the following equation:

$$\mathrm{C/No} = \frac{(\mathrm{T_d} R_0(\tau).\mathrm{sinc}(\Delta f_c T_d))^2}{L_n N_0 + J(\mathrm{T_d.C_j.sinc(T_d.\Delta f_i)})^2} \quad 30$$

where:

N_0 is the thermal noise power (Watts)

28 A. T. Balaei, A. G. Dempster and J. Barnes, A Novel Approach in Detection and Characterization of CW Interference of GPS Signal using Receiver Estimation of C/No, 2006), 1120-1126.

29 A. T. Balaei, J. Barnes and A. G. Dempster, "Characterization of Interference Effects on GPS Signal Carrier Phase Error" (Melbourne, Australia: Spatial Science Institute, Proceedings of SSC 2005 Spatial Intelligence, Innovation, Praxis: The national biennial Conference of the Spatial Science Institute, September 2005).

30 Balaei, Dempster and Barnes, A Novel Approach in Detection and Characterization of CW Interference of GPS Signal using Receiver Estimation of C/No, 1120-1126

L_n is the processing gain in the noise (unitless)

T_d is the integration duration time (seconds)

τ is the signal-reference code phase difference in code chips (degrees)

Δf_c is the actual carrier frequency minus the estimate of the carrier frequency (Hz)

Δf_i is the actual interference frequency minus the estimate of the interference frequency (Hz)

J is the interference power (Watts)

C_j is the j^{th} spectral line coefficient

$R_0(\tau)$ is the cross correlation of the received C/A code and the receiver replica of the same code.

The calculation of the actual C/No ratio is obtained by the narrow-to-wideband power ratio method. In extremely over-simplified operational-speak, this method determines the C/No ratio as an expression which basically divides the average narrowband power over the accumulation interval by the average wideband power over the interval. Using this information, the measured carrier power-to-noise density as a function of the power ratio measurement can be determined to be:

$$c/n_0 \approx \frac{M}{\tau}\frac{\overline{P}_{N/W}-1}{M-\overline{P}_{N/W}} \quad 31$$

where $\overline{P}_{N/W}$ is the ratio of the average narrow band power to the average wideband power

τ is the accumulation interval

M is the sub-intervals of τ

Figure 16 depicts the plot of an experiment which illustrates the relative agreement between the theoretical C/No and the actual C/No with a slight offset due to

31 Balaei, Dempster and Barnes, A Novel Approach in Detection and Characterization of CW Interference of GPS Signal using Receiver Estimation of C/No, 1120-1126

the lack of clarity on the unknowns, specifically the interference power. Referring back to the mathematical expression for the *theoretical* C/No it can be readily observed that other than the frequency of the interference, there are three other parameters: signal power, background noise power, and interference power. The first two of these parameters are known for the given operating environment. We know what the signal power should be from a GPS satellite and we know what the background noise power should be when we take into account the operating environment. What we don't readily know yet is the interference power. Interference power can be estimated from the AGC level in the RF front-end.[32] Once this is known we can have the *theoretical* C/No approximate the *actual* C/No as closely as possible. This enables the ability to have the least amount of difference between the two calculations at the frequency where the interference exists. Therefore, the frequency where there is the least amount of difference between the two C/No's is the frequency where the interference is occurring.

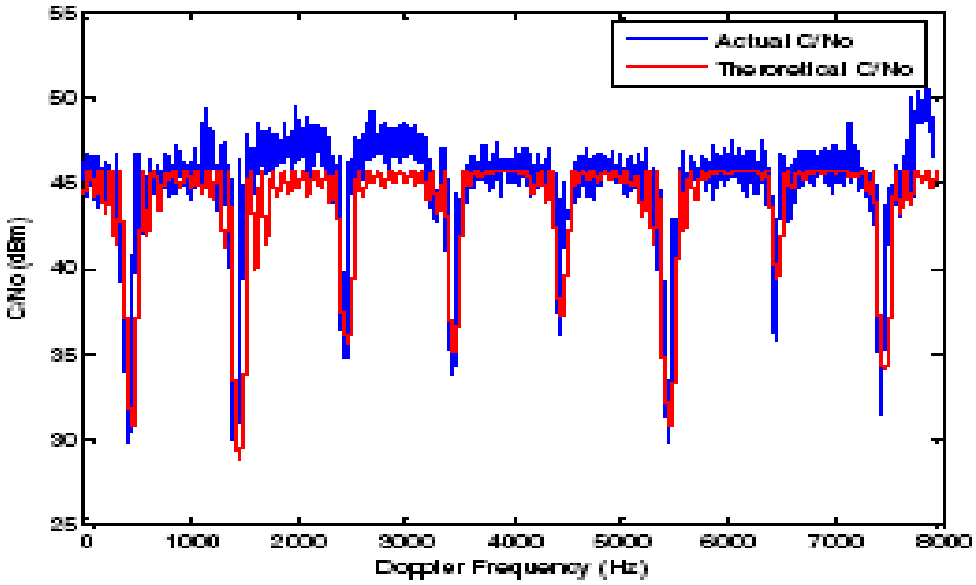

Figure 16. C/No plots calculated using both the parametric[theoretical] method and the power ratio (actual) method (From Balaei, Dempster, and Barnes)[33]

32 F. Bastide, Christophe Macabiau and DM Akos, "Automatic Gain Control (AGC) as an Interference Assessment Tool" 2003.

33 Balaei, Dempster and Barnes, A Novel Approach in Detection and Characterization of CW Interference of GPS Signal using Receiver Estimation of C/No, 1120-1126

The previous six methods have illustrated some of the most familiar and effective ways to identify that interference is occurring on a GPS signal. We are also interested in determining the location of the interfering source so that actions can be taken to eliminate it. We'll now examine some of the most common methods of localization of an interfering signal.

B. LOCALIZATION

1. Carrier/Noise (C/N_O) Jammer Location Sensor

This is a very basic method of estimating jammer location. This approach takes the Carrier to Noise Ratio (C/No) data from the GPS receiver and logs it with respect to satellite signal strength and position and time data from the receiver. One of the main benefits to this approach is that no additional special purpose GPS user equipment is needed since most GPS receivers already generate this information. One of the major drawbacks to this method is that it depends on large variations of C/No ratios as a function of distance from jammer. When low power jammers are used the C/No variation is not that large so this approach lacks the ability of identifying accurate jammer locations. Figure 17 illustrates the simplicity of how a C/No Jammer Location Sensor would work in a networked environment.

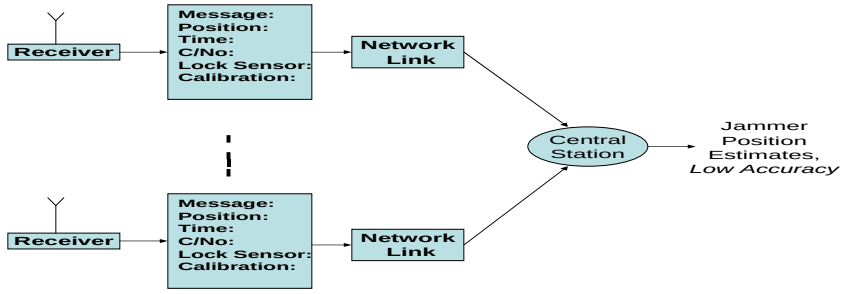

Figure 17. C/No Sensor Architecture (After Brown, Reynolds, Roberts, & Serie)[34]

34 Brown and others, Jammer and Interference Location System - Design and Initial Test

This approach takes time-correlated data from numerous receivers and networks all of this information together and compiles it at a central station. The central station then estimates jammer position based upon precisely known locations in the area and then compares this information to their reported locations. Based on the C/N_o ratio an estimate is made as to the location of the jamming source.

2. Angle of Arrival (AOA) Jammer Location Sensor

This method of jammer location is accomplished with standard GPS user equipment that is integrated with a Controlled Radiation Pattern Antenna (CRPA) that is capable of detecting jammer signals. The CRPA places a null in the antenna pattern in the direction of the jammer by using the detected AOA of the interfering signal. A form of triangulation is used to determine jammer location by taking various readings of AOA as the equipment outfitted with GPS conducts its movements. Although this type of information can be obtained from numerous GPS systems and then fed into a centralized processing system to estimate jammer location, the advantage of this approach is that it can be accomplished with only one system which is moving to triangulate in on the interfering signal. Figure 18 depicts how an aircraft might use this type of system to identify a jammer location.

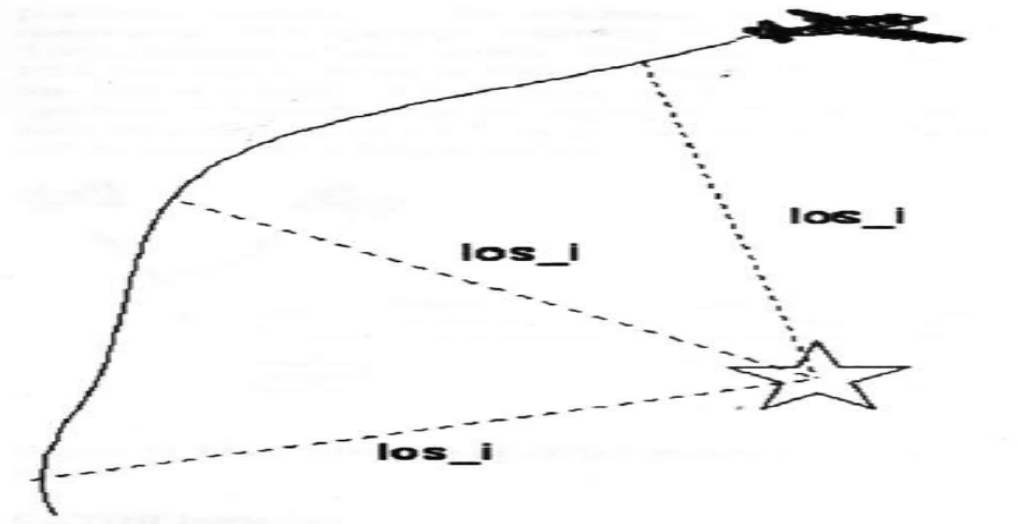

Figure 18. Aircraft using AOA and triangulation to locate jammer source (From Brown, Reynolds, Roberts, & Serie)[35]

One disadvantage of this approach is that its accuracy is limited as a function of the pointing accuracy of the null it provides. For a single receiver, the accuracy is also affected by the inertial heading accuracy of the equipment it is associated with.

3. Time Difference of Arrival (TDOA) Jammer Location Sensor

This method of locating GPS jammers is more accurate than the two previously mentioned approaches. The TDOA approach first involves the separating out of the jammer signal from the actual GPS signal. The jammer signal is then measured in a synchronized manner using the GPS signal to get highly accurate timing information from two or more receivers simultaneously while the GPS receivers are moving. The analysis of the amount of time it takes for the jammer signal to reach the receiver can then be used to find the distance from the jammer to the receiver. Using this information for several different locations of at least three (ideally four) receivers yields a highly accurate triangulation picture which accurately estimates where the jamming source is emanating from in three dimensions.

35 Brown and others, Jammer and Interference Location System - Design and Initial Test

Wikipedia, although not necessarily always highly regarded in the academic and research circles, does provide a succinct and useful version of how multilateration in conjunction with TDOA measurements yields highly accurate locations of emitters. Here is a portion of that presentation:

Consider an emitter at unknown location (x,y,z) that we wish to locate. Consider also a multilateration system comprising four receiver sites at known locations: a central site, C, a left site, L, a right site, R and a fourth site, Q. The travel time (T) of pulses from the emitter at (x,y,z) to each of the receiver locations is simply the distance divided by the pulse propagation rate (c):

$$T_L = \frac{1}{c}\left(\sqrt{(x-x_L)^2+(y-y_L)^2+(z-z_L)^2}\right)$$

$$T_R = \frac{1}{c}\left(\sqrt{(x-x_R)^2+(y-y_R)^2+(z-z_R)^2}\right)$$

$$T_Q = \frac{1}{c}\left(\sqrt{(x-x_Q)^2+(y-y_Q)^2+(z-z_Q)^2}\right)$$

$$T_C = \frac{1}{c}\left(\sqrt{(x-x_C)^2+(y-y_C)^2+(z-z_C)^2}\right)$$

If the site C is taken to be at the coordinate system origin,

$$T_C = \frac{1}{c}\left(\sqrt{x^2+y^2+z^2}\right)$$

Then the time difference of arrival between pulses arriving directly at the central site, and those coming via the side sites, can be shown to be:

$$\tau_L = T_L - T_C = \frac{1}{c}\left(\sqrt{(x-x_L)^2+(y-y_L)^2+(z-z_L)^2} - \sqrt{x^2+y^2+z^2}\right)$$

$$\tau_R = T_R - T_C = \frac{1}{c}\left(\sqrt{(x-x_R)^2+(y-y_R)^2+(z-z_R)^2} - \sqrt{x^2+y^2+z^2}\right)$$

$$\tau_Q = T_Q - T_C = \frac{1}{c}\left(\sqrt{(x - x_Q)^2 + (y - y_Q)^2 + (z - z_Q)^2} - \sqrt{x^2 + y^2 + z^2}\right)$$

where $(x_L,\ y_L,\ z_L)$ is the location of the left receiver site, etc, and c is the speed of propagation of the pulse, often the speed of light. Each equation defines a separate hyperboloid. The multilateration system must then solve for the unknown target location (*x*,*y*,*z*) in real time. All the other symbols are known.[36]

Another point to be made here is that multilateration is generally much more accurate than triangulation due to the fact that it is much easier to measure time accurately than it is to form the narrow beams necessary for triangulation. Appendix B provides a much more thorough and developed derivation of position determination using TDOA of GPS satellite signals. The derivation in Appendix B chooses to use four equations and four unknowns, partially because there are guaranteed to be four satellites in view of the horizon for any point on the earth, and mostly because adding a fourth equation allows for the ability to reach simple and satisfactory solutions due to the elimination of the square root terms which the inclusion of the fourth equation provides.

36 Wikipedia contributors, "Multilateration," Wikipedia, The Free Encyclopedia, http://en.wikipedia.org/wiki/multilateration?oldid=228786716 (accessed 8 June 2008).

THIS PAGE INTENTIONALLY LEFT BLANK

IV. PLANNING CONSIDERATIONS FOR CONDUCTING GPS JAMMING

The fact of land-based jamming being impeded by terrain and other obstacles are very relevant and useful pieces of information when it comes to the task of actually testing a GPS jammer within the continental United States. Figure 19 illustrates the magnitude of impact that even a 0.5-watt GPS Jammer could have on a metropolitan area.

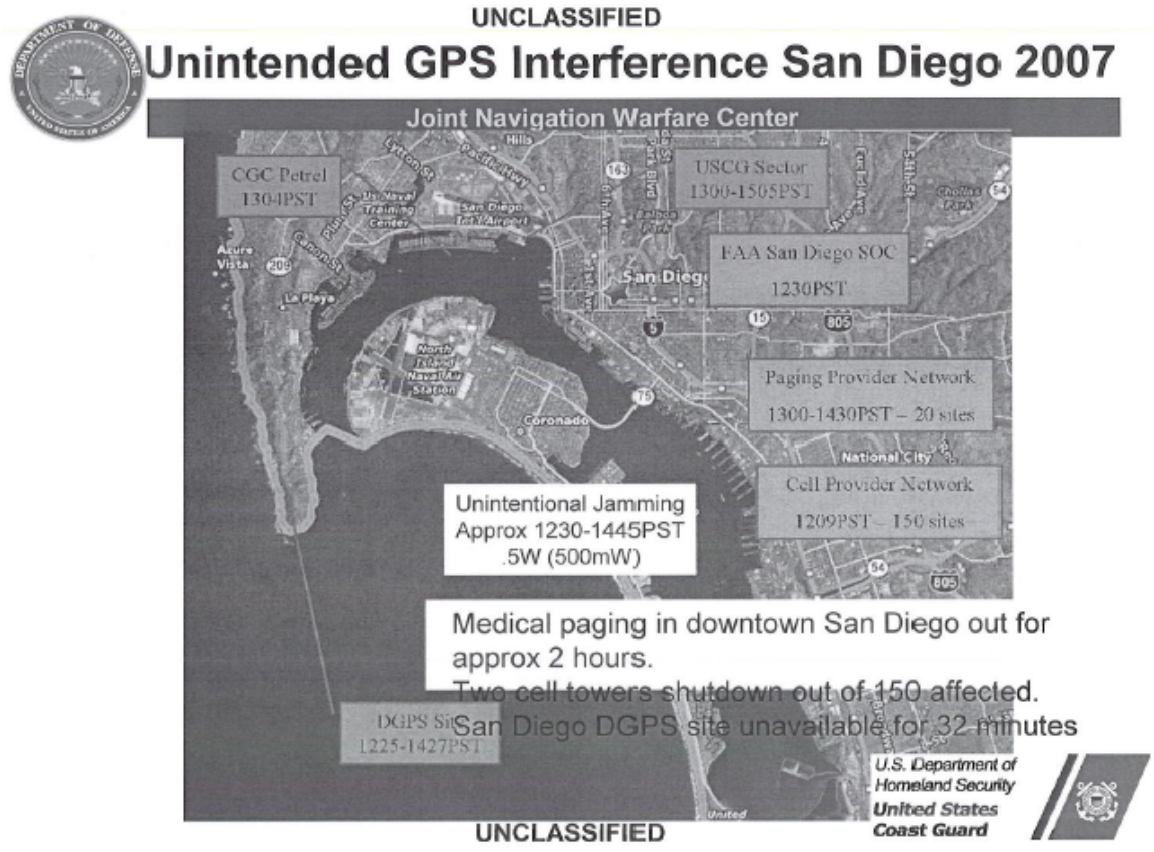

Figure 19. Unintended GPS Interference in a metropolitan area (From JNWC-Navwar-Threat Overview Brief)[37]

37 Haseloff, JNWC-Navwar-Threat Overview Brief (Unclassified Portion) United States Army FA-40 Symposium, 1-2-30

Contrary to wishful thinking, one is not allowed to just haphazardly go about "testing" their GPS jammer wherever and whenever they want. As a matter of fact, the requirements and approval process to conduct this type of testing can be extremely detailed and require an enormous amount of lead-time in order to legally conduct the tests.

> GPS is used extensively by the civilian community in commerce and science. Some examples of civilian GPS applications include use as a timing source for utilities and science, tracking devices for the transportation industry, quality assurance tools for agriculture, and navigation systems for civil aviation. Additionally, GPS is used for its original, intended application — military systems. In each of these uses, one commonality exits: the requirement for noninterference of the user community due to DoD testing.[38]

Figure 20 gives a very general frequency clearance process for conducting GPS jamming within the continental United States. Frequency clearance is essential when one considers that this type of jamming is actually affecting the signal from the GPS satellite and therefore would affect numerous military and civilian activities if not properly managed beforehand. Looking at the routing in Figure 20 one can quickly surmise that it would require copious amounts of time to work the GPS jamming request through all of the necessary approval authorities. If this were the only way that GPS jamming could be conducted then at least there would be a consistent approach to attacking this requirement.

> Unfortunately, specific processes for obtaining GPS jamming clearances vary extensively from base-to-base, and even within bases. The process of obtaining a frequency clearance at some facilities is no different than if one wished to install a two-way radio in a truck. Other ranges require extensive analysis (such as jamming footprint studies) and documentation.[39]

38 Matt Boggs and Kenea C. Maraffio, Mitigation Paths for Free-Space Jamming (China Lake, California: GPS/INS Systems Section, Naval Air Warfare Center Weapons Division (NAWCWPNS), http://www.fas.org/spp/military/program/nav/gpsjam.pdf (accessed 17 July 2008).

39 Ibid.

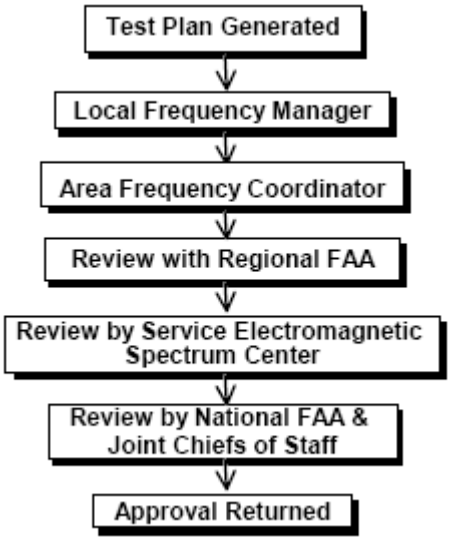

Figure 20. Generic GPSJ [GPS Jamming] Approval Process (From Boggs and Maraffio)[40]

For our purposes here in Monterey, California one of the closest and most logical choices where one might even consider conducting GPS Jamming out in the open would be at Fort Hunter Liggett which is about an hour and a half away by car. Appendix A provides a copy of their Training Support Request (TSR) form which illustrates the first two stages of Figure 20, which are coming up with a testing plan and then submitting that plan for approval through the local frequency manager.

In order to come up with a valid testing plan for GPS Jamming one of the necessary prerequisites is to understand not only the power output of GPS Jammers but also the proper method with which to employ them to cause minimal impact upon other GPS users. One of the ways to do this with GPS Jamming signals is to use jammers with directional antennas instead of omni-directional jammers. Directional antennas afford the opportunity to continue with meaningful and realistic jamming scenarios while minimizing the likelihood that GPS users external to the testing will be affected. Directional antennas/emitters, as the name implies, allow the user to direct the signal in

40 Matt Boggs and Kenea C. Maraffio, Mitigation Paths for Free-Space Jamming (China Lake, California: GPS/INS Systems Section, Naval Air Warfare Center Weapons Division (NAWCWPNS), http://www.fas.org/spp/military/program/nav/gpsjam.pdf, (accessed 17 July 2008).

the direction that they would like. Figure 21 shows the horizontal radiation pattern for a typical Directional Jammer. In this Figure the primary lobe, the one with the greatest propagation, is directed due North with a 20º horizontal beamwidth (10º to either side of 0º). The secondary lobes on either side of the primary lobe have much less propagation range than the primary but can still be oriented as needed.

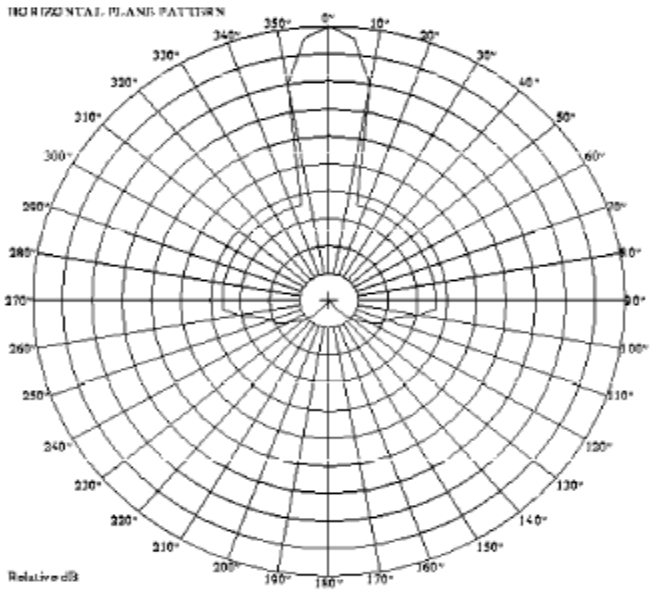

Figure 21. Horizontal Radiation Pattern for Directional Jammer (From Boggs and Maraffio)[41]

Directional Jammers when coupled with proper terrain selection can provide significant mitigation capabilities when it comes to containing GPS Jamming signals. Knowing that you have a Directional Jammer you must also perform a reconnaissance of prospective jammer testing areas to ensure that adequate terrain, buildings, etcetera are available to act as a shield against the jamming signal. This approach was taken for the planned jammer testing at Fort Hunter Liggett. A standard 1:50,000 terrain map of Fort Hunter Liggett was initially used in concert with the locations of available Training Areas provided by Range Control, to get a sense of potential GPS Jammer testing sites. Once

41 Matt Boggs and Kenea C. Maraffio, Mitigation Paths for Free-Space Jamming (China Lake, California: GPS/INS Systems Section, Naval Air Warfare Center Weapons Division (NAWCWPNS), http://www.fas.org/spp/military/program/nav/gpsjam.pdf, (accessed 17 July 2008).

several Training Areas were selected the reconnaissance then turned to the very useful and relatively new reconnaissance tool known as Google® Earth. Google® Earth was used to zoom in on actual satellite images of the training areas in order to develop a greater appreciation for the available terrain. The program was used to identify possible terrain features, like mountains for example, which could be used as a backstop for any GPS jamming. The mountain would be the direction that the Directional GPS Jammer would be pointed at. If possible, the side lobes of the signal propagation would be oriented in such a manner to make maximum effective use of available terrain to act as shielding.

THIS PAGE INTENTIONALLY LEFT BLANK

V. JAMMING DEVICE

Effective testing and evaluation of a GPS interference detection system requires that it be subjected to a jamming signal, matching the GPS L1 signal in frequency and bandwidth. To that end, this chapter is dedicated to the construction and testing of a portable low power GPS jamming device. The jamming device design was originally published in "Phrack" online magazine, and the design has now proliferated around the World Wide Web. Figure 22 illustrates the schematic diagram for the jamming device.

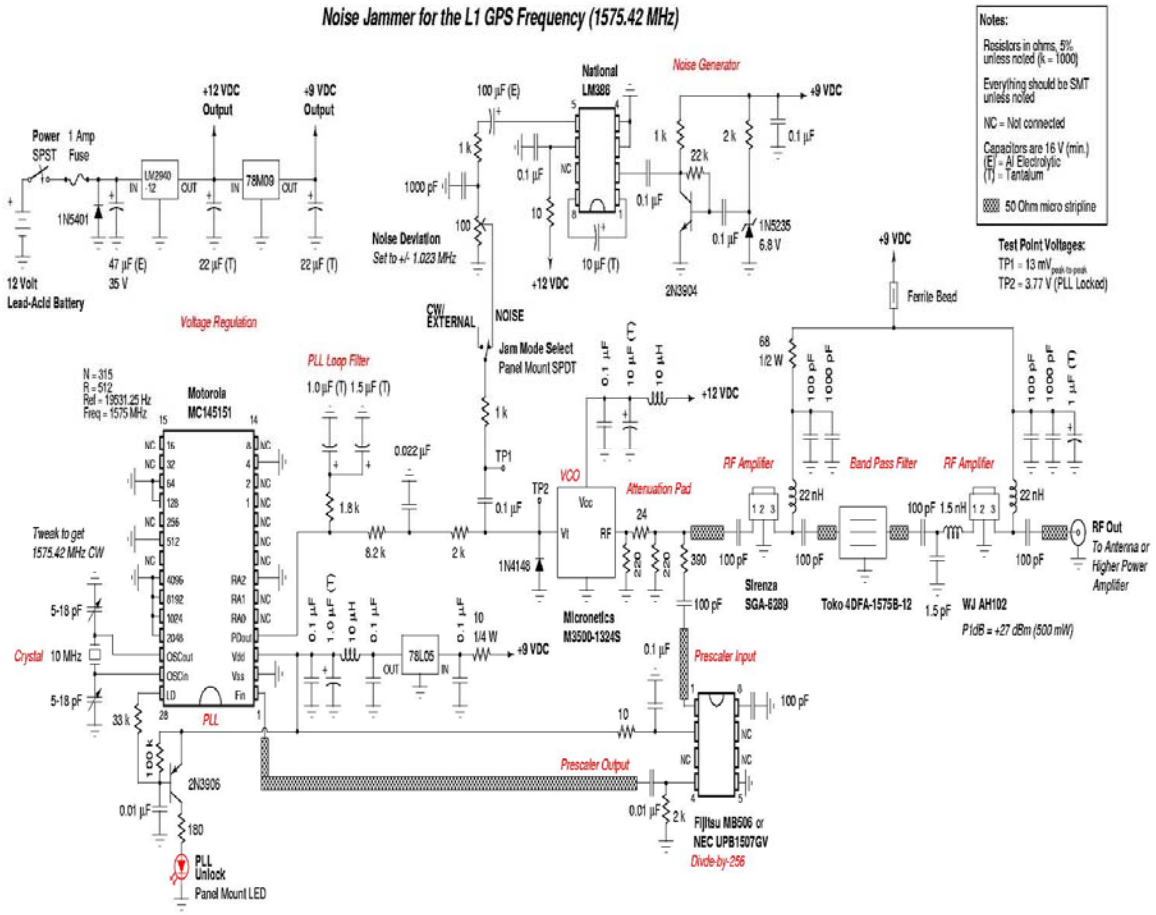

Figure 22. Original Jamming Device Schematic[42]

42 Green Bay Professional Packet Radio, "Noise Jammer for the L1 GPS Frequency (1575.42 MHz)," http://www.qsl.net/n9zia/, (accessed 19 September 2008).

The circuit diagram was implemented using a professional schematic capture and layout software suite called PCB123©. Using the PCB123© schematic program the components of the circuit were connected as illustrated in Figure 23.

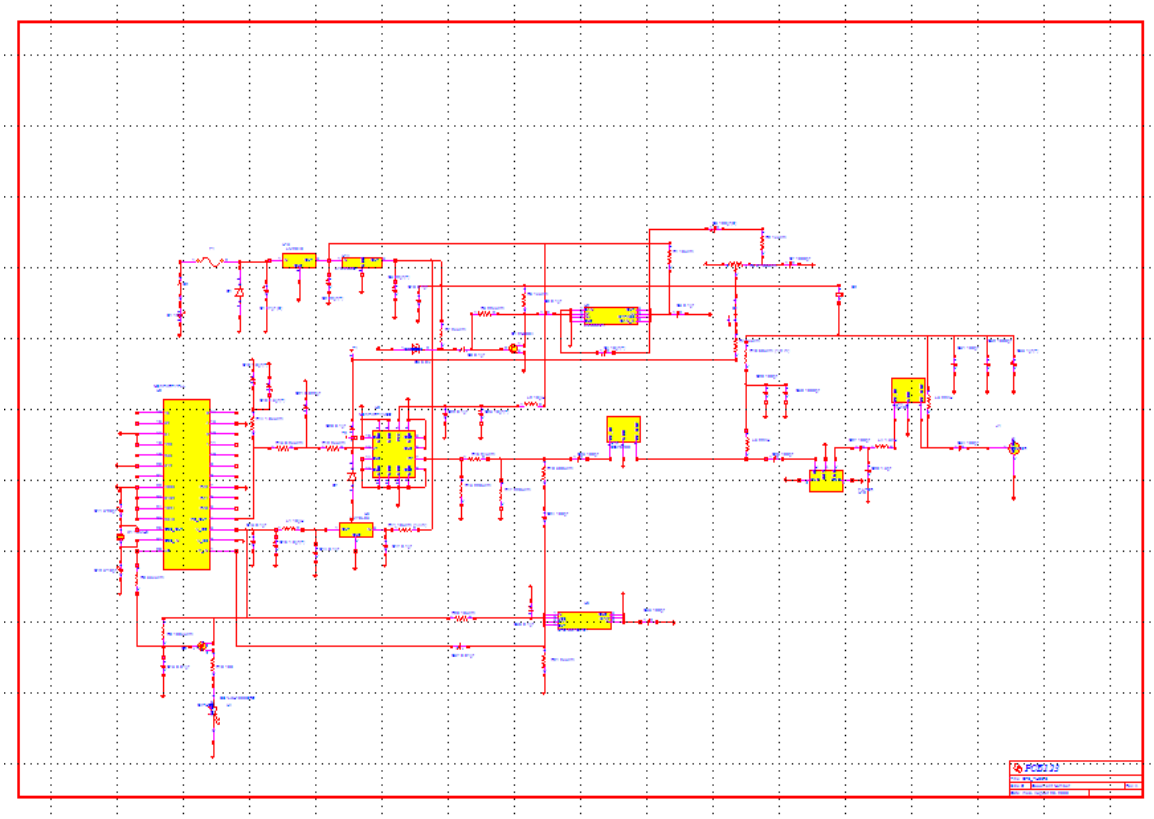

Figure 23. Jamming Device Component Connections in PCB123© Schematic Program

One of the difficulties encountered in using the PCB123© schematic program is that several of the components used in circuit were not available as standard library parts. Although the problem was eventually overcome by using the build part utility to create the required components, the process was extremely time intensive. There were also multiple instances in which the program crashed and had to be reinstalled to recover the schematic file. Once the schematic was complete, the resulting file was saved and converted into a netlist. The netlist file maintains a list of all the components, their package types, as well as the interconnections between them.

Once completed, the schematic and its associated net list are exported to the PCB123© layout program. Unfortunately, the exported components and the wires connecting them do not maintain the spatial integrity established in the schematic program. A visual comparison of Figure 23 and Figure 24 below illustrates how the components look before and after the export.

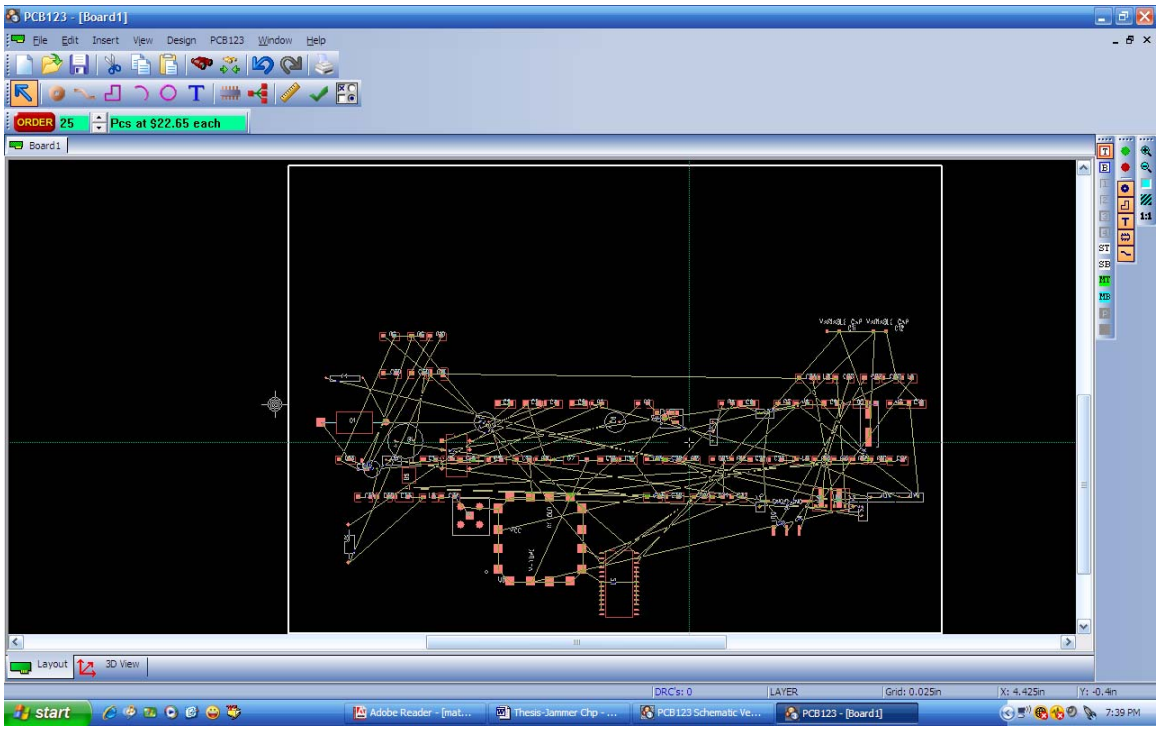

Figure 24. Screenshot of Netlist Export to PCB Layout©

After the export, the obligatory tasks are to rearrange the components in a logical manner and commence the wire routing process. Generally, components are positioned to reflect the arrangement of the original schematic. This is a common practice that facilitates troubleshooting and makes it easier follow signal paths through components.

One of the critical tasks associated with building a layout for a circuit which operates at microwave frequencies is determining the dimensions of the microstrip lines. Microstrip lines are wire traces that propagate the RF signal from one component to another. The dimensions of the microstrip lines in an RF design determine the desired characteristic impedance. The specified characteristic impedance for the jamming device

is 50 ohms. A simple formula for calculating the characteristic impedance of a microstrip line is given by: $Zo = \frac{87}{\sqrt{\varepsilon + 1.41}} \ln\left(\frac{5.98h}{0.8w + t}\right)$[43]

In this equation, Zo is the characteristic impedance in ohms, ε is dielectric constant, and w, t, and h are the width, thickness and height in millimeters of the copper trace above the ground plane, respectively. Figure 25 shows a cross-sectional sketch of a microstrip line mounted on a printed circuit board.

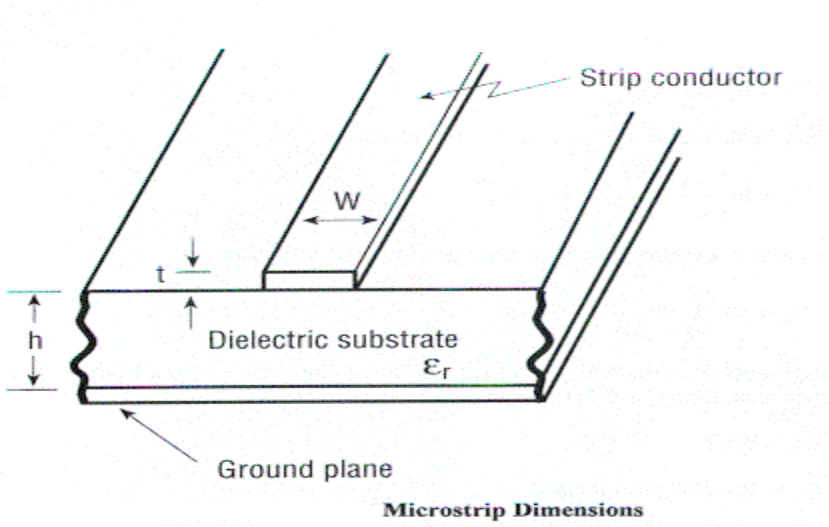

Figure 25. Dimensions of PCB Mounted Microstrip Line[44]

> Microstrip transmission line is a kind of "high grade"printed circuit construction, consisting of a track of copper or other conductor on an insulating substrate. There is a "backplane" on the other side of the insulating substrate, formed from similar conductor. Looked at end on, there is a "hot" conductor which is the track on the top, and a "return" conductor which is the backplane on the bottom. Microstrip is therefore a variant of 2-wire transmission line. If one solves the electromagnetic equations to find the field distributions, one finds very nearly a completely TEM (transverse electromagnetic) pattern. This means that there are only a few regions in which there is a component of electric or magnetic field in the direction of wave propagation. The quasi TEM pattern arises

43 Green Bay Professional Packet Radio, "Microstripline Analysis & Design Results," http://my.athenet.net/~multiplx/cgi-bin/strip.cgi, (accessed 19 September 2008).

44 Ibid.

> because of the interface between the dielectric substrate and the surrounding air. The electric field lines have a discontinuity in direction at the interface. The boundary conditions for electric field are that the normal component (i.e. the component at right angles to the surface) of the electric field times the dielectric constant is continuous across the boundary; thus in the dielectric which may have dielectric constant 10, the electric field suddenly drops to 1/10 of its value in air.[45]

The actual dimensions for the jamming device's microstrips were determined with an online calculator. This web-based application requires only that one specify the dielectric constant and the characteristic impedance. The remaining parameters for the microstrips are autonomously calculated for the user. Figure 26 below displays the results for the jamming device's microstrips. The values specified for the dielectric constant and characteristic impedance are 4.8 and 50 ohms.

```
Operating frequency : 2450.000 MHz
Dielectric constant : 4.800
Effective dielectric constant : 3.595
Substrate thickness : 1.500 mm (0.059 inches / 59.055 mils)


Microstripline impedance : 50.000 ohms
Microstripline physical width : 2.777 mm (0.109 inches / 109.349 mils)
Velocity factor : 0.523
Velocity of propagation : 0.456
One wavelength (360°) : 64.041 mm (2.521 inches / 2521.306 mils)
Quarter wavelength (90°) : 16.010 mm (0.630 inches / 630.327 mils)
```

Figure 26. Results of Online Microstrip Calculator[46]

The final layout for the printed circuit board was completed with microstrip specifications annotated in Figure 26. Figures 27 and Figure 28 show the final layout and the actual printed circuit board produced.

45 David Jeffries, "What is Microstrip Transmission Line?" http://personal.ee.surrey.ac.uk/Personal/D.Jefferies/mstrip.html, (accessed 19 September 2008).

46 Green Bay Professional Packet Radio, Microstripline Analysis & Design Results .

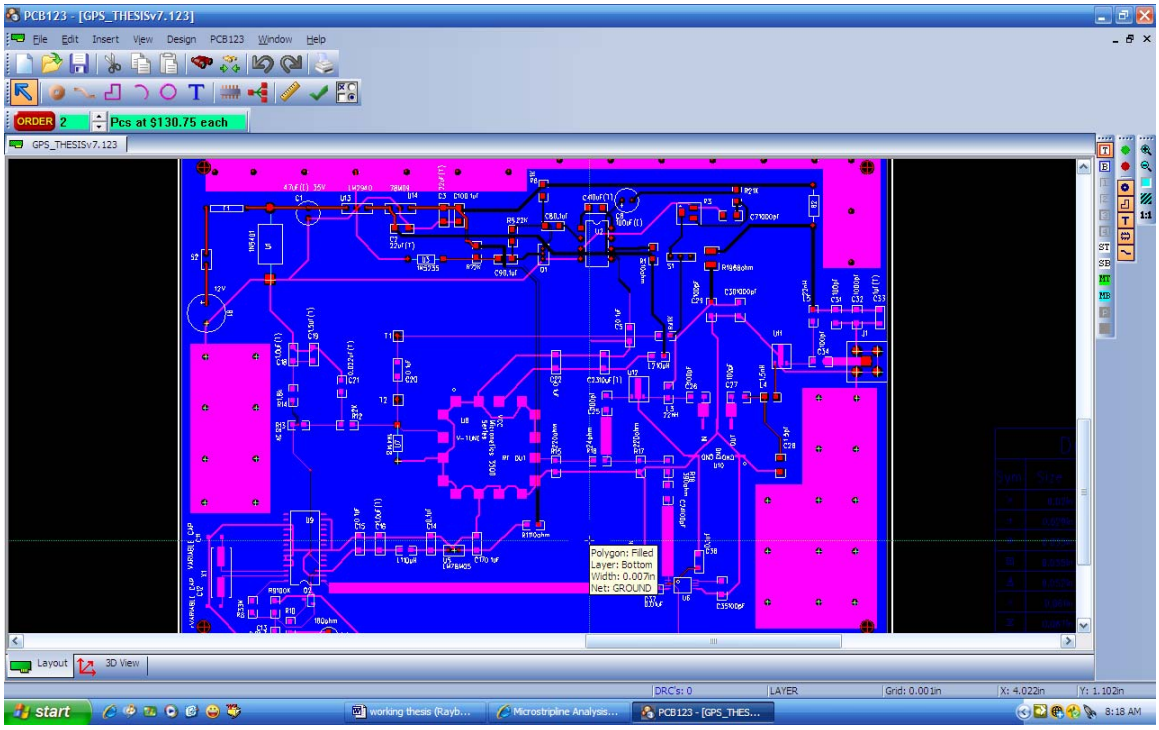

Figure 27. Screenshot of Final PCB Layout©

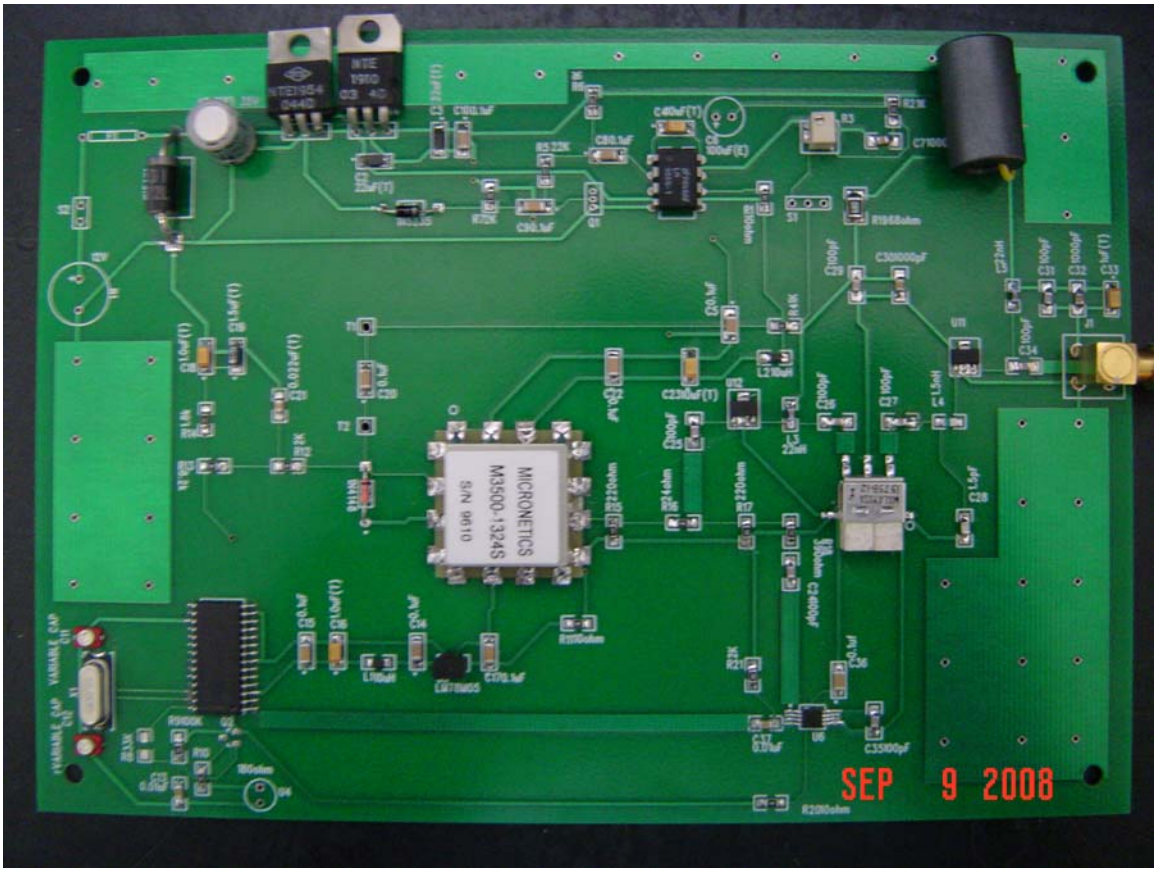

Figure 28. Printed Circuit Board Produced Using PCB Layout©

The jamming device is comprised of three major sections. First is the power section, which provides the interface for the 12-volt battery that runs the system. Next is the noise generator. This section provides the "static" which interferes with the pseudo-random noise (PRN) codes transmitted by the orbiting GPS satellites. Finally, the radio frequency (RF) section uses frequency modulation to mix the noise signal with the 1575.42 MHz L1 carrier frequency, and then subsequently radiates the modulated carrier through an antenna.

A. THE POWER SECTION

As mentioned previously, the power section contains a 12-volt rechargeable battery, which provides a steady flow of energy to the jamming device. However, like many unregulated portable power supply devices, the Powerflex© model 8SPA measures

slightly higher than its advertised 12 volts when fully charged. Figure 29 shows the measured terminal voltage supplied by the battery.

Figure 29. Battery's Measured Terminal Voltage

The 13.6 volts supplied by the battery exceeds the supply voltages required by the integrated circuit components in the noise generator and RF sections. The noise generator section has a single integrated circuit that requires nine volts for proper operation. However, the RF section contains three integrated circuits, two of which require only five volts. The third integrated circuit component in the RF section, the voltage controlled oscillator (VCO), is the only component in the jamming device which requires 12 volts.

The various voltage levels demands for the RF and noise generator sections is achieved with the use of three-terminal voltage regulators. Each voltage regulator has an input, output, and ground terminal. The task of a voltage regulator is to take a higher voltage that is applied to its input terminal and produce the desired regulated voltage at the output terminal. The regulated output terminal voltage is fixed at the value specified by the manufacturer for the particular model in use. For our jamming device, the regulated output terminal voltages are 12, 9, and 5 volts respectively. The battery along with the three voltage regulators is connected in a cascaded fashion as indicated in Figure 30.

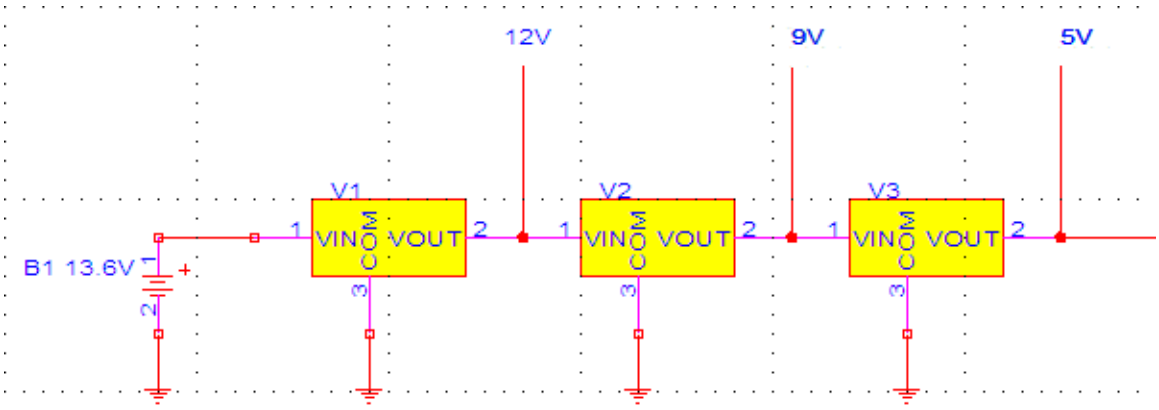

Figure 30. Major Components in Power Section

In Figure 30, the battery's 13.6-volt positive terminal is attached to the input of the 12-volt regulator. The regulator's 12-volt output becomes the input to the 9-volt regulator. The final regulator receives the 9-volt input and produces the final 5-volt output to complete the voltage distribution network.

B. THE NOISE GENERATOR SECTION

The key components in this section are the LM386 audio amplifier, the 6.8-volt zener diode, and a 2N3904 bipolar junction transistor. The operation of the noise generator begins by reverse biasing the zener diode. The zener diode is designed to operate in this reverse bias region once the zener potential of 6.8 volts has been reached. The zener diode produces low amplitude noise signals up to 100 MHz. The noise signal

is subjected to further processing via the LM386 audio amplifier. The LM386 amplifies and filters the signal for subsequent injection into the RF section through a variable resistor and capacitor network. The oscillator will use this noise signal to modulate the L1 carrier frequency. Figure 31 shows a schematic representation of the components in the noise section.

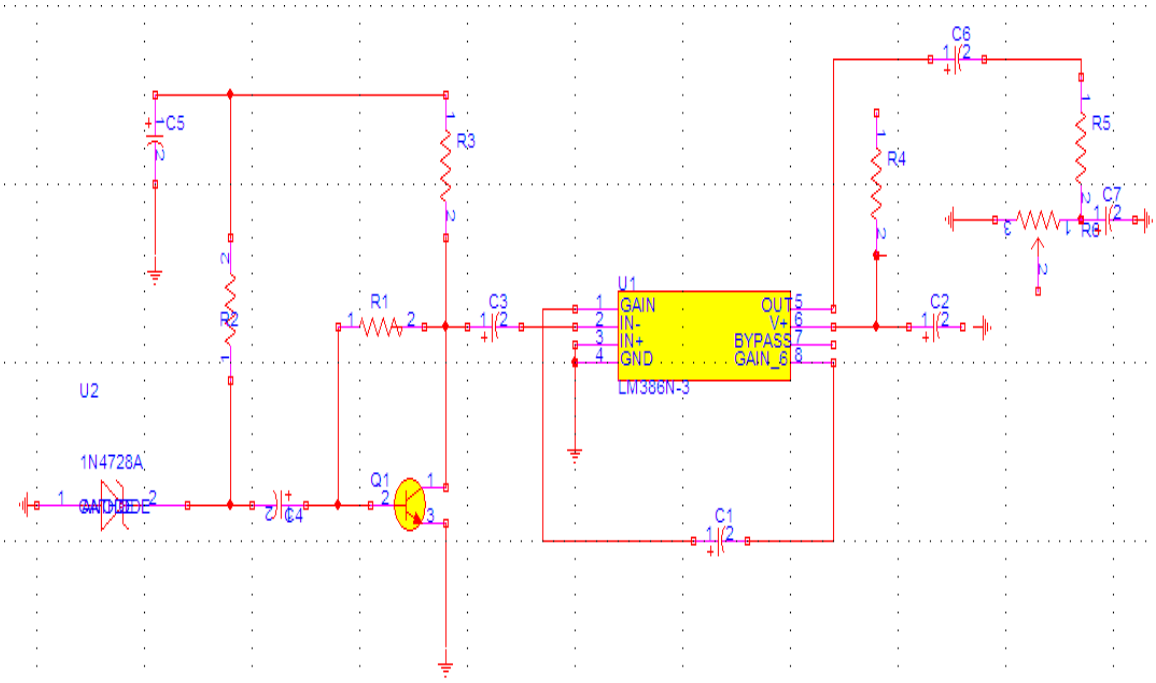

Figure 31. Major Components in Noise Section

C. THE RADIO FREQUENCY SECTION

The final section of the jamming device is the radio frequency section. The function of the RF section is to produce the L1 carrier frequency and modulate the carrier with the noise signal. The significant components comprising this section are the voltage controlled oscillator, the phase lock loop (PLL), and the prescaler.

The voltage controlled oscillator, phase lock loop, and prescaler form a closed loop system that synthesize the carrier frequency. To begin the process, the phase lock loop's oscillator input is driven with a 10 MHz reference frequency derived from a quartz crystal. Inside the phase lock loop, the 10 MHz reference frequency is divided 512 times

by the chip's internal counter circuitry. This produces a new reference frequency of 19531.25 Hz. The new reference frequency will be used for comparison to the frequency output of the prescaler.

Initially, the voltage controlled oscillator produces an output frequency in response to a direct current voltage applied to its voltage tuning input. A resistive network first attenuates the output signal's voltage level. Once the VCO's output voltage is reduced by the attenuator network, a portion of the signal is fed into the prescaler, where its frequency is divided by 256 and passed to the phase lock loop. At the PLL, the VCO signal's frequency is divided by 315. The resulting frequency quotient is then compared to the 19531.25 Hz reference frequency.

During the comparison process, the phase lock loop attempts to validate that the two signals have the same frequency and phase. If both signals match in frequency and phase, the phase lock loop applies a direct current voltage to the VCO's tuning input. The direct current voltage at the tuning input again drives the VCO's output frequency where the process begins anew and continues indefinitely.

In the event that the reference frequency and the VCO's output frequency do not match, the phase lock loop will attempt to compensate for the difference. If the VCO's frequency is higher than 19531.25 Hz reference, the phase lock loop will make every effort to lower the VCO's frequency to 19531.25 Hz and achieve phase lock. The phase lock loop will attempt to raise the VCO's frequency if it is below the 19531.25 Hz reference.

The phase lock condition can be verified through one of several outputs on the PLL. The most readily available method is to observe the status of the phase detector output pin using an oscilloscope. When the reference frequency and VCO input frequency are matched, phase lock is achieved, and the phase detector output pin will display a steady direct current voltage on the oscilloscope. However, if the VCO frequency is higher, an oscilloscope will display a series of negative pulses, and a series of positive pulses if it is lower. Figure 32 illustrates the positive pulses detected at the phase detector output indicating lack of phase lock.

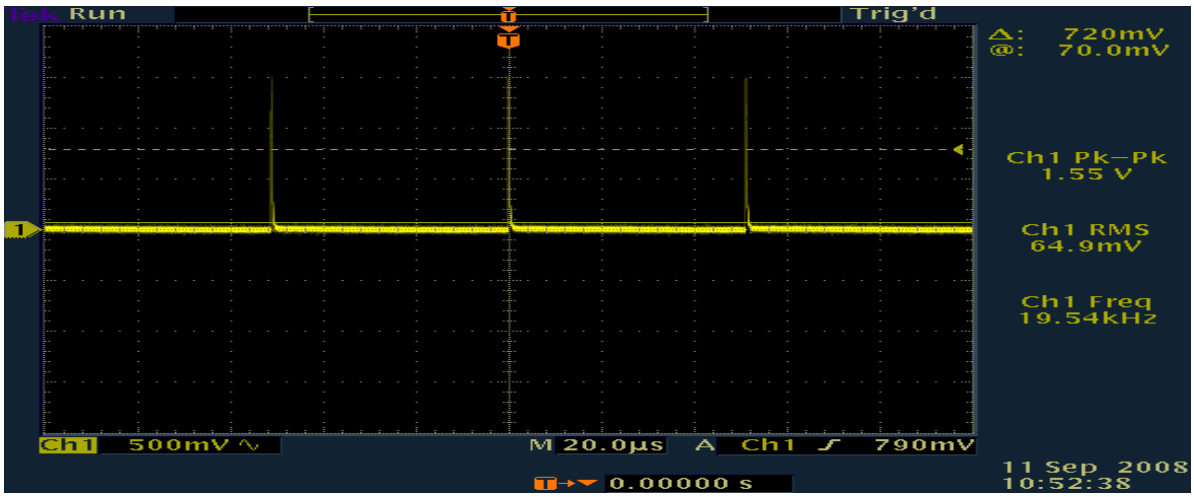

Figure 32. Positive pulses at phase detector output indicating lack of phase lock

VI. DETECTOR AND LOCATION SYSTEM ARCHITECTURE

In order to contend with the threat posed by portable GPS jamming devices, an architecture must be established to facilitate the detection and location of electromagnetic interference. Collectively, the components of the architecture should allow for one or more of the localization techniques described in the previous chapter to be implemented. The specific functions inclusive to the architecture must encompass:

- RF sensing
- Data logging
- Terrain mapping
- GPS signal-to-noise monitoring

These functions outlined above can be implemented with combinations of commercially available hardware and software. The use of commercial products is more practical than a bottom up approach to designing the necessary hardware and software components. The task that lies ahead for the remainder of this chapter is identifying commercial products that will allow the architecture to be realized.

A. RF SENSING

The RF sensor is the most critical component in the architecture. The sensor component will be the "eyes and ears" of the system and will provide the capability to detect electromagnetic interference within the bandwidth of interest. Specifically, the sensing requirement calls for a component that can detect 1575.42 MHz RF carriers as well as any accompanying modulating signal.

The Digital Scout© is a commercially available frequency counter capable of detecting RF signals from 10 – 2600 MHz. The unit can internally store up to 1000 detected frequencies or alternatively, log the captured frequencies to an external device via serial bus interface. In addition, it also logs data on the relative signal strength of detected signals. The Digital Scout's© resolution bandwidth ratings are 100 Hz and 1kHz. The resolution bandwidth specification is important since detection of interference

signals requires that an RF sensor have resolution bandwidth down to 1 kHz or less at either the L1 frequency or at the intermediate frequency. Figure 33 illustrates the Digital Scout® frequency counter.

Figure 33. The Digital Scout® handheld frequency counter (From Optoelectronics®)

The Digital Scout® also comes with accompanying software to facilitate external data logging. However, as an alternative, Classic Business Technologies® offers a software suite designed to work with Optoelectronics® products. The Classic Business Technologies® suite offers more data logging features than the standard package included with the Digital Scout®. Figure 34 shows an example of data that can be logged by the OptoSuite Pro® software.

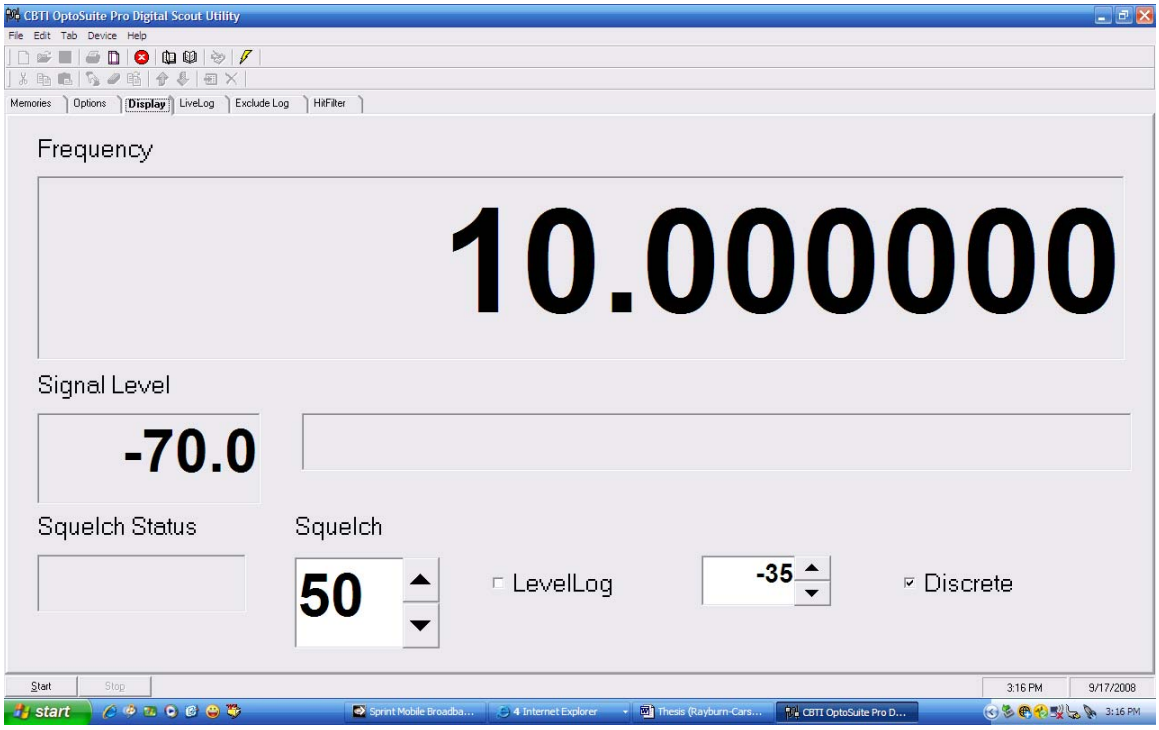

Figure 34. Screenshot showing some data logging features available in Classic Business Technologies OptoSuite Pro® software

B. DATA LOGGING

The data logging component of the architecture is fairly simple. This component can be implemented with either a portable laptop computer, or a Personal Digital Assistant (PDA) type device. The primary requirement for data logger is that is must possess sufficient memory, and be accommodate the software demands for the architecture.

C. TERRAIN MAPPING

This feature of the architecture will co-exist with the data logger as a software package. The purpose of terrain mapping software is to provide an interactive digital map that will assist in geo-locating a potential EMI source. The mapping software

should allow the user to plot coordinates as well as determine range and bearing between coordinates. Google® Earth is well renowned software package that possesses these features.

D. GPS SIGNAL-TO-NOISE MONITORING

The GPS signal-to-noise ratio (S/N) monitoring feature is a critical component of the architecture. The ability to monitor and assess changes in the GPS S/N will provide a means of correlating significant drops in S/N with incidences of L1 carrier frequency detections picked up by the RF sensor. Many commercial GPS receivers support this capability through the National Marine Electronics Association (NMEA) communications protocol. Using the NMEA protocol and serial interface cable, an NMEA enabled GPS receiver can be connected to the data logger. The data logger can be used to interrogate the GPS receiver with NMEA sentences to extract its internally logged information about the receiver's S/N. Figure 35 shows the syntax for entering NMEA sentences.

```
$GPGSV,2,1,08,01,40,083,46,02,17,308,41,12,07,344,39,14,22,228,45*75

Where:
      GSV          Satellites in view
      2            Number of sentences for full data
      1            sentence 1 of 2
      08           Number of satellites in view

      01           Satellite PRN number
      40           Elevation, degrees
      083          Azimuth, degrees
      46           SNR - higher is better
           for up to 4 satellites per sentence
      *75          the checksum data, always begins with *
```

Figure 35. Using a NMEA sentence to extract S/N information from a GPS receiver[47]

47 Dale DePriest, "NMEA Data," http://www.gpsinformation.org/dale/nmea.htm (accessed 22 September 2008).

THIS PAGE INTENTIONALLY LEFT BLANK

VII. CONCLUSIONS AND RECOMMENDATIONS

Although this thesis was not able to fully meet the initial lofty goals of Designing, Building, and Testing a Handheld GPS Interference Detector, much progress in the groundwork towards that endeavor has been achieved. In hindsight, trying to accomplish this much technical sophistication by two Space System *Operators* in a very short timeframe while simultaneously taking courses, was definitely a bridge too far. But, having said that, much research and design has been accomplished which can be used to drive this goal further down the road to fruition.

The disadvantaged tactical warfighter who is forward deployed requires the capability to gain actionable intelligence when his GPS environment encounters a jamming situation. The warfighter needs to be to quickly ascertain the difference between when he is indeed being jammed and when it is nothing more than his GPS enabled equipment or munitions that have malfunctioned. He also needs the ability to learn exactly where that interference is coming from so that he can determine if it is malicious or not and then take the appropriate action to terminate the interference. These forward deployed warfighters at the tip of spear in harms way often do not have the time to wait for the large, detailed analysis conducted by organizations far from them both physically and mentally. There are several AF TENCAP programs currently on-going now that still do not provide the capability to provide this type of information immediately and autonomously to the disadvantaged warfighter on the front line. These warfighters do not have the ability to pack a computer with SIPRNET capability to access certain sites to try to determine what has happened to their GPS signal and even if they did this is not something which they should have to search for. The bottom-line is that this is the type of information that must be pushed forward to individuals depending on the accuracy of GPS instead of being pulled after a problem has been encountered and solutions are being sought after.

The fact still remains that currently in the war zones and for the foreseeable future there will continue to be sources of interference which impede or totally degrade GPS signals to the point which renders GPS munitions and equipment inoperable. According to the vast majority of recent reports coming from the war zone, the current sources of GPS interference are for the most part self-inflicted interference by friendly forces. This interference appears to be mostly due to errant communication devices transmitting at incorrect frequencies or the harmonics of certain transmissions frequencies which coincide with the L-band frequencies of GPS.

This thesis has provided an overview of six of some of the most recent and common approaches to detecting GPS jamming whether that jamming is pulsed or CW: Correlator Output Power, Variance of Correlator Output Power, Carrier Phase Vacillation, Active Gain Control (AGC) Control Loop Gain, Multiple-Model Adaptive Estimation (MMAE), and Receiver Estimation of C/No. Several of these approaches are facets of other approaches and when used in conjunction with other methods provide a more accurate characterization of the interference.

The issue of localization of the jammer location has also been addressed through the three approaches of: Carrier/Noise (C/No) Jammer Location Sensor, Angle of Arrival (AOA) Jammer Location Sensor, and Time Difference of Arrival (TDOA) Jammer Location Sensor. The most accurate of these is the TDOA method because it relies on the highly reliable nanosecond timing of the cesium clocks on-board GPS satellites. This approach based on highly accurate timing is markedly more accurate than the triangulation approach which requires extremely narrow beamwidths to be pointed over vast distances between the satellites in MEO and the receivers on the ground.

The Decision was made to design, build, and test a low-powered GPS Jammer from a design easily obtained off of the Internet. This approach was chosen because it was deemed to be a realistic choice considering that a common threat of the United States for the foreseeable future appears to be terrorist elements. It was thought that they would be much more likely to try to gain an asymmetric advantage by using open source GPS Jammer designs rather than invest the time, money, and infrastructure required to develop the larger and more powerful GPS Jammers. Also, by building their own jammers they

would be able to rid themselves of the necessity to purchase GPS jammers which might make their possible intentions able to be more easily tracked and denied. This approach was also chosen because we too could not just go out and purchase a GPS Jammer off of the street and even if we could the cost of even small jammers would be prohibitive for the available money that we would have at our disposal.

Unfortunately, even after numerous attempts and trouble shooting over a considerable timeframe, we were unable to get our GPS Jammer to produce the desired frequency to jam the GPS L1 Frequency (1575.42 MHz). Achieving this fundamental benchmark was crucial to the follow-on work of testing the jammer effective ranges. It was also critical for the intended analysis of the jamming on the GPS signal for the civilian Garmin GPS receiver and the military's Precision Lightweight Ground Receiver (PLGR). All coordination had been made for training areas and obtaining PLGRs for testing. Without an operable jammer we were unable to conduct the field tests of detecting and locating the jamming source.

We recommend that any future work towards this endeavor pick-up where we left off. A lot of time and effort was put into learning how to use the PCB software which allowed us to design the PCB boards and have them professionally manufactured. This measure was taken to minimize the probability that something might be poorly constructed by two novice electronic technicians. In the process of meticulously soldering all of the surface-mounted extremely tiny capacitors, resistors, conductors, etcetera, we have graduated from novice solderers to journeyman solderers. Recommend that any future work begin with continued testing of the GPS Jammer boards to ascertain why the correct frequency is not being generated. Once this gets accomplished then the testing of the jammers effective ranges and the identification and localization of the jamming can be examined using some of the methods described in this thesis.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX A

This appendix provides an example of a blank Training Support Request (TSR) to conduct any type of training on Fort Hunter Liggett, California. The purpose of providing this form here is to illustrate and corroborate some of the initial requirements for conducting GPS Jamming. Although this form is not specifically for GPS Jamming, it does capture the requirement to provide a detailed test plan (Concept of Operations) and to request the clearance of any frequencies that will be used, i.e., 1575.42 MHz for L1 GPS jamming.

FORT HUNTER LIGGETT TRAINING SUPPORT REQUEST (TSR) FORM

NOTE: Units must complete the TSR. Incomplete TSR's will result in a delay of scheduling. Previous TSR editions are obsolete. Only personnel listed below are authorized to make changes.

Due to current construction projects, areas requested are subject to change.

Submit TSR and supporting documents via email to the Training Division: RangeOps2@liggett-emh1.army.mil Commercial phone numbers are: (831) 386-2510/2310/3145. DSN: 686-2510/2310/3145. If unable to email, please fax to (831) 386-2766 or mail to: Commander, CSTC, Ft Hunter Liggett, ATTN: AFRC-FMH-DTS, Jolon, CA 93978-7111. Email is the preferred method of submission. Please call to confirm receipt of TSR and any documents that are sent.

1. General Unit Information

A. Unit:		**Date TSR Submitted:**	
B. Unit Higher Headquarters:		**Component:** USAR, ARNG, USN, USNR, USMC, Other (specify)	
C. Unit Identification Code (UIC):		**DoD Activity Address Code (DODAAC):**	
D. Primary Point of Contact:		**Alternate Point of Contact:**	
Phone:		**Phone:**	
Fax:		**Fax:**	
Email:		**Email:**	
E. Unit Mailing Address: Include Zip Code, Office Symbol			
F. Type of Training: Annual Training, MUTA 4, MUTA 5, Other (explain)			
G. Personnel/Vehicle/Aircraft Strength:			
	DATE / TIME	**Officers M/F**	**Enlisted M/F**
Arrival Advance Party			
Arrival Main Body			
Departure Main Body			
Departure Rear Detachment			
Types of Vehicles	**Vehicle Quantity**	**Types of Aircraft**	**Aircraft Quantity**

H. Unit Training/Operations Objectives: (Individual MOS Training, Weapons Qualification, FTX, LFX, CLFX, FCX, CPX, TEWT, etc.)
NOTE Unit must provide:
(1) Concept of operations and training objectives.
(2) Overlays (convoy routes, foot marches, dig plans, obstacle plans, smoke/obscurant operations, surface danger zone diagrams, etc.) that support the training or live-fire exercise. These documents must be received before you will be allowed to sign for any training site or facility.
(3) Appointment Orders for OIC's and RSO's. Land Usage Briefings are given on Fridays at 1400 Hours at Range Control. Units are required to read, understand and comply with FHL 350-2 prior to conducting training.

2. Scheduling of Facilities. All facilities and support will be requested and scheduled by the Training Division.

A. Training Area and Facility Requests. All training area and range requests are controlled by the Training Division (Bldg S-320 Range Control). Check each Training Area or Facility required and provide the training dates and times for the occupation of those areas. **Only request areas that will be used. Requesting a facility does not give you the TA unless so requested. Provide Actual Training or Firing Dates and Times for each area being requested.**

		Arrival Date / Time	Departure Date / Time
	TA 1		
	TA 2		
	North Land Nav Course		
	NBC Chamber		
	TA 3		
	TA 4		
	TA 5		
	TA 6		
	Crocker Range		
	TA 6B		
	TA 7		
	TA 8		
	TA 9		
	TA 10		
	TA 11		
	TA 12A		
	Horton DZ		
	TA 12B		
	TA 12C		
	TA 13E		
	East Land Nav Beginner		
	East Land Nav Intermediate		
	TA 13W		
	25 Meter Zero Range		
	KD Automated Record Fire Range		

	Combat Pistol Qualification Range		
	Confidence Obstacle Course		
	Conditioning Obstacle Course		
	Rappel Tower		
	TA 14		
	TA 15		
	EPW Training Site		
	Convoy Live Fire Range (SDZ affects TAs 15,16,19,20,21,24)		
	Convoy Blank Fire Course (TAs 15, 20, 24)		
	Patricia Drop Zone		
	TA 16		
	TTB 8J		
	Area 8J Buildings		
	TA 16B		
	Pugil Pit		
	Bayonet Assault Course		
	Hand Grenade Inert Assault Course		
	Rope Bridge Site		
	Schoonover Tactical Assault Airstrip		
	TTB Schoonover		
	Miller Shower Point		
	Lower Blackjack (Area around shower)		
	TA 17		
	TA 18		
	TA 19		
	TA 20		
	Demolition Site / Engineer Construction		
		Arrival Date / Time	Departure Date / Time
	TA 21		
	TA 22		
	MPRC Ammo Holding Area		
	Machine Gun Range, MPRC		
	Main Tank Tower, MPRC		
	M203 Range, MPRC		
	B9 Range, MPRC (Firing points set-up for 25 meter Zero)		
	Hand Grenade HE Range, MPRC		
	TA 23		
	TA 24		
	TA 25*		
	TA 26		
	Palisades Rappel Site		
	TA 27		
	MOUT Site		
	South Land Nav Course		
	TTB Ward		
	TA 28		
	TA 29		
	88M Test Course (Main Gate Area)		
	Drown Proofing Facility (Post Fitness Center Pool)		
	TUSI Heliport		
	Drop Zone/Landing Zone		
	Post Theater (350 Pax)		

*** Environmental restrictions apply to TA 25. Environmental Review required for any activity**.

B. Billeting Request: Include the Quantity by Male and Female Bays or Rooms, Arrival and Departure dates and times.

FACILITY	Quantity of Male/Female	Arrival Date/Time	Departure Date/Time
40-Person Open Bay			
2-Person Rooms			
Admin Office Areas			

3. Specialized Support Requests. All specialized requests must be coordinated with the Training Division. Provide a Memorandum to the Training Division requesting the support needed. All requests must be submitted by Training Division unless otherwise noted.

Email: RangeOps2@liggett-emh1.army.mil Commercial phone numbers are: (831) 386-2510/2310/3145. DSN: 686-2510/2310/3145. If unable to email, please fax to (831) 386-2766 or mail to: Commander, CSTC, Ft Hunter Liggett, ATTN: AFRC-FMH-DTS, Jolon, CA 93978-7111. Email is the preferred method of submission. Please call to confirm receipt of any documents that are sent. The Training Division will task the Ft Hunter Liggett Directorates to provide the support requested. Indicate support requests needed by checking the appropriate box and providing additional memorandums for each required service. Failure to do so will result in a delay of coordinated support.

☐ **Chemical Latrines:** USAR units must provide a Latrine Request if needed. All other entities must contract a latrine provider directly and arrange for delivery and payment. A list of providers will be provided if requested.

☐ **Ice request:** Provide a memo with quantity and type requested, date and time for pick-up.

☐ **POL Support:** FHL offers retail and bulk fuel capacities of JP-8, MOGAS and other POL products. Memos must include DODAAC, fuel type, estimated quantity and number of fuel keys.

☐ **DOL Vehicle Support:** DOL has a limited number of administrative vehicles which are issued on a reimbursable basis. Provide a memo for request and method of payment Amount of reimbursable will be dependent upon request.

☐ **Telecommunications Support:** FHL controls computer interface, field phone hook-ups (MAGDROPS), frequency usage and other communications services. Provide a memo with specific support requirements.

☐ **Radio Frequency:** Units must submit a frequency request for any radios, communications or electronic equipment.

☐ **Radio Support:** Units must provide their own FM radio support. A limited number of hand-held radios are available. Provide a memo for type of radio support requested, along with quantity requested.

☐ **Integrated Training Area Management (ITAM):** Soldier Field Cards, environmental awareness briefings, pre-exercise planning (avoiding sensitive cultural & natural resources), GPS/GIS. Located in Bldg 331, phone x-2305, Email: Art.Hazebrook@liggett-emh1.army.mil

☐ **Environmental Support:** Activities described in FHL 350-2 require environmental clearance or for hazardous waste. Submit Environmental Reviews to the Training Division Not Later Than 45 days prior to training.

☐ **Dining Facility Support:** FHL Dining Facility can feed up to 960 people per meal. Mermites and UGR's are also available (Chow, Box lunch, Beverages, Mermites, MRE's, Organizational meals). Memos must be submitted 30 days in advance with projected headcount and feeding plan. Phone (831) 386-3520. Email: Justine.Brooks1@us.army.mil

☐ **Billeting:** Provide a current DA 1687 for individuals to draw billets. If linen is requested, provide a memo for quantity. Phone: (831) 386-2644/2075. Email: FHLBilletRequest@liggett-emh1.army.mil

☐ **Arms Room:** Units must provide the Access Roster a minimum of 14 days prior to the codes being issued. Roster will contain at least 2, but not more than 6 names, time period needed and the Commander's signature. Access codes will be picked up at LEA upon arrival. Email requested to FHLBilletRequest@liggett-emh1.army.mil

☐ **MWR Support:** For the Post Pool, Gym, Picnic grounds, etc, provide memo with the dates and supported requested. Contact the MWR manager Mr Tertulien at (831) 386-2910. Email: Charlemagne.Tertulien@liggett-emh1.army.mil

☐ **Religious Support:** If support is requested, contact the Chapel in Bldg 190, (831) 386-2808/2465. Fax: x-3102.

☐ **Ammunition Supply Point (ASP):** FHL contains a fully functional ASP for issue and turn-in. Hours of operation are 0730-1630 Hours, Monday thru Friday. All ammunition must be coordinated with FHL ASP. Submit DA 581 to the ASP in Bldg S-723, phone (831) 386-2614, Email: quasas@liggett-emh1.army.mil

Note: To draw ammunition, all units must bring their DA 581 to be signed and approved by the Training Division prior to drawing.

☐ **Equipment Concentration Site (ECS-170):** The DCSLOG, 63rd RSC, USARC manages and controls the equipment from ECS. Units must first contact the ECS Site Manager and determine the availability of equipment (vehicles, radios, etc) and make initial coordination. Phone (831) 386-2213/3598/2801/2770. Email: ECS170@us.army.mil

☐ **AAFES/Commissary:** If AAFES support is requested, call (831) 385-4585, Bldg 80. If Commissary support is requested, call 386-2190, Bldg 83.

☐ **Transient Lodging Requirements:** Available for TDY and temporary stays. For reservations, contact the Lodging Office in Bldg 196. Phone (831) 386-2511/2108

FAD and MIPR Requirements: Mailing address for all Finance Authorization Documents (FAD) (USAC units) or Military Interdepartmental Purchase Requests (MIPR):

US Army Combat Support Training Center
Attn: Resource Management Office
Bldg 312, 9th Street
Dublin, CA 94568

POC: Ms Laura Orozco
Commercial Phone: (925) 875-4423
Fax: (925) 875-4424
Email: Laura.Orozco@usar.army.mil

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX B

This appendix expounds upon, in much greater detail, the actual mathematical calculations necessary to locate a signal using Time Difference of Arrival (TDOA). The algorithm is developed for simultaneously solving four equations and four unknowns which represent the distances to/from any four satellites that are guaranteed to be in the horizon of any location on earth.[48] In their article, "A synthesizable VHDL Model of the Exact Solution for Three-Dimensional Hyperbolic Positioning System," Ralph Bucher and D. Misra methodically derive and develop the necessary equations for determining positions of mobile elements on the earth by using the TDOA information of the satellite signals.

48 Ralph Bucher and D. Misra, "A Synthesizable VHDL Model of the Exact Solution for Three-Dimensional Hyperbolic Positioning System," VLSI Design 15, no. 2 (3 October 2001, 2002), 507-520.

version will utilize the IEEE numeric_std package so it can be synthesized into an ASIC by anyone seeking a hardware implementation.

THE ALGORITHM

The essence of the TDOA technique is the equation for the distance between two points.

$$d = \sqrt{(x_2 - x_1)^2 + (y_2 - y_1)^2 + (z_2 - z_1)^2} \quad (1)$$

The distance between a mobile and a station is determined indirectly by measuring the time it takes for a signal to reach the station from the mobile. Multiplying the TOA t by the signal velocity c gives us the distance d. From now on, R will be used to represent the distance d since it is the more commonly used notation in TDOA literature.

We need to solve for the three unknowns x, y and z (mobile position). Therefore, Eq. (1) is expanded to three equations when the specific locations of three satellites i, j and k are given. This requirement can be easily met since GPS satellites broadcast their exact locations.

$$ct_i = R_i = \sqrt{(x_i - x)^2 + (y_i - y)^2 + (z_i - z)^2} \quad (2)$$

$$ct_j = R_j = \sqrt{(x_j - x)^2 + (y_j - y)^2 + (z_j - z)^2} \quad (3)$$

$$ct_k = R_k = \sqrt{(x_k - x)^2 + (y_k - y)^2 + (z_k - z)^2} \quad (4)$$

where, x_i, y_i, z_i, x_j, y_j, z_j and x_k, y_k, z_k are the position of ith, jth and kth satellite, respectively and these positions vary with time.

Unfortunately, solving the three equations for three unknowns will not lead to a simple and satisfactory solution because of the square root terms. The solution can be simplified by adding another satellite l for an additional equation. In addition, the accuracy of the mobile position will be further improved if four equations are used. This requirement is easily met since four GPS satellites are guaranteed to be in the horizon of any location on earth [9]. The four equations will be combined to form expressions for time difference of arrivals (TDOAs) R_{ij}, R_{ik}, R_{kj} and R_{kl}.

$$R_i - R_j = R_{ij} = \sqrt{(x_i - x)^2 + (y_i - y)^2 + (z_i - z)^2} - \sqrt{(x_j - x)^2 + (y_j - y)^2 + (z_j - z)^2} \quad (5)$$

$$R_i - R_k = R_{ik} = \sqrt{(x_i - x)^2 + (y_i - y)^2 + (z_i - z)^2} - \sqrt{(x_k - x)^2 + (y_k - y)^2 + (z_k - z)^2} \quad (6)$$

$$R_k - R_j = R_{kj} = \sqrt{(x_k - x)^2 + (y_k - y)^2 + (z_k - z)^2} - \sqrt{(x_j - x)^2 + (y_j - y)^2 + (z_j - z)^2} \quad (7)$$

$$R_k - R_l = R_{kl} = \sqrt{(x_k - x)^2 + (y_k - y)^2 + (z_k - z)^2} - \sqrt{(x_l - x)^2 + (y_l - y)^2 + (z_l - z)^2} \quad (8)$$

Moving one square root term to the other side gives us:

$$R_{ij} - \sqrt{(x_i - x)^2 + (y_i - y)^2 + (z_i - z)^2} = -\sqrt{(x_j - x)^2 + (y_j - y)^2 + (z_j - z)^2} \quad (9)$$

$$R_{ik} - \sqrt{(x_i - x)^2 + (y_i - y)^2 + (z_i - z)^2} = -\sqrt{(x_k - x)^2 + (y_k - y)^2 + (z_k - z)^2} \quad (10)$$

$$R_{kj} - \sqrt{(x_k - x)^2 + (y_k - y)^2 + (z_k - z)^2} = -\sqrt{(x_j - x)^2 + (y_j - y)^2 + (z_j - z)^2} \quad (11)$$

$$R_{kl} - \sqrt{(x_k - x)^2 + (y_k - y)^2 + (z_k - z)^2} = -\sqrt{(x_l - x)^2 + (y_l - y)^2 + (z_l - z)^2} \quad (12)$$

Squaring both sides produces the following set of equations:

$$R_{ij}^2 - 2R_{ij}\sqrt{(x_i - x)^2 + (y_i - y)^2 + (z_i - z)^2} + (x_i - x)^2 + (y_i - y)^2 + (z_i - z)^2 = (x_j - x)^2 + (y_j - y)^2 + (z_j - z)^2 \quad (13)$$

$$R_{ik}^2 - 2R_{ik}\sqrt{(x_i - x)^2 + (y_i - y)^2 + (z_i - z)^2} + (x_i - x)^2 + (y_i - y)^2 + (z_i - z)^2 = (x_k - x)^2 + (y_k - y)^2 + (z_k - z)^2 \quad (14)$$

$$R_{kj}^2 - 2R_{kj}\sqrt{(x_k - x)^2 + (y_k - y)^2 + (z_k - z)^2} + (x_k - x)^2 + (y_k - y)^2 + (z_k - z)^2 = (x_j - x)^2 + (y_j - y)^2 + (z_j - z)^2 \quad (15)$$

$$R_{kl}^2 - 2R_{kl}\sqrt{(x_k - x)^2 + (y_k - y)^2 + (z_k - z)^2} + (x_k - x)^2 + (y_k - y)^2 + (z_k - z)^2 = (x_l - x)^2 + (y_l - y)^2 + (z_l - z)^2 \quad (16)$$

Expanding the squared terms to the left of the square root term produces:

$$R_{ij}^2 - 2R_{ij}\sqrt{(x_i - x)^2 + (y_i - y)^2 + (z_i - z)^2} + x_i^2 - 2x_i x + x^2 + y_i^2 - 2y_i y + y^2 + z_i^2 - 2z_i z + z^2 = x_j^2 - 2x_j x + x^2 + y_j^2 - 2y_j y + y^2 + z_j^2 - 2z_j z + z^2 \quad (17)$$

$$R_{ik}^2 - 2R_{ik}\sqrt{(x_i - x)^2 + (y_i - y)^2 + (z_i - z)^2} + x_i^2 - 2x_i x + x^2 + y_i^2 - 2y_i y + y^2 + z_i^2 - 2z_i z + z^2 = x_k^2 - 2x_k x + x^2 + y_k^2 - 2y_k y + y^2 + z_k^2 - 2z_k z + z^2 \quad (18)$$

$$R_{kj}^2 - 2R_{kj}\sqrt{(x_k - x)^2 + (y_k - y)^2 + (z_k - z)^2} + x_k^2 - 2x_k x + x^2 + y_k^2 - 2y_k y + y^2 + z_k^2 - 2z_k z + z^2 = x_j^2 - 2x_j x + x^2 + y_j^2 - 2y_j y + y^2 + z_j^2 - 2z_j z + z^2 \quad (19)$$

$$R_{kl}^2 - 2R_{kl}\sqrt{(x_k - x)^2 + (y_k - y)^2 + (z_k - z)^2} + x_k^2 - 2x_k x + x^2 + y_k^2 - 2y_k y + y^2 + z_k^2 - 2z_k z + z^2 = x_l^2 - 2x_l x + x^2 + y_l^2 - 2y_l y + y^2 + z_l^2 - 2z_l z + z^2 \quad (20)$$

Eliminating the x^2, y^2 and z^2 terms reduces the equation set to:

$$R_{ij}^2 - 2R_{ij}\sqrt{(x_i - x)^2 + (y_i - y)^2 + (z_i - z)^2} + x_i^2 - 2x_i x + y_i^2 - 2y_i y + z_i^2 - 2z_i z = x_j^2 - 2x_j x + y_j^2 - 2y_j y + z_j^2 - 2z_j z \quad (21)$$

$$R_{ik}^2 - 2R_{ik}\sqrt{(x_i - x)^2 + (y_i - y)^2 + (z_i - z)^2} + x_i^2 - 2x_i x + y_i^2 - 2y_i y + z_i^2 - 2z_i z = x_k^2 - 2x_k x + y_k^2 - 2y_k y + z_k^2 - 2z_k z \quad (22)$$

$$R_{kj}^2 - 2R_{kj}\sqrt{(x_k - x)^2 + (y_k - y)^2 + (z_k - z)^2} + x_k^2 - 2x_k x + y_k^2 - 2y_k y + z_k^2 - 2z_k z = x_j^2 - 2x_j x + y_j^2 - 2y_j y + z_j^2 - 2z_j z \quad (23)$$

$$R_{kl}^2 - 2R_{kl}\sqrt{(x_k - x)^2 + (y_k - y)^2 + (z_k - z)^2} + x_k^2 - 2x_k x + y_k^2 - 2y_k y + z_k^2 - 2z_k z = x_l^2 - 2x_l x + y_l^2 - 2y_l y + z_l^2 - 2z_l z \quad (24)$$

Shifting all but the square root term to the right and combining similar terms produces:

$$\sqrt{(x_i - x)^2 + (y_i - y)^2 + (z_i - z)^2} = [R_{ij}^2 + x_i^2 - x_j^2 + y_i^2 - y_j^2 + z_i^2 - z_j^2 + 2x_j x - 2x_i x + 2y_j y - 2y_i y + 2z_j z - 2z_i z]/2R_{ij} \quad (25)$$

$$\sqrt{(x_i - x)^2 + (y_i - y)^2 + (z_i - z)^2} = [R_{ik}^2 + x_i^2 - x_k^2 + y_i^2 - y_k^2 + z_i^2 - z_k^2 + 2x_k x - 2x_i x + 2y_k y - 2y_i y + 2z_k z - 2z_i z]/2R_{ik} \quad (26)$$

$$\sqrt{(x_k - x)^2 + (y_k - y)^2 + (z_k - z)^2} = [R_{kj}^2 + x_k^2 - x_j^2 + y_k^2 - y_j^2 + z_k^2 - z_j^2 + 2x_j x - 2x_k x + 2y_j y - 2y_k y + 2z_j z - 2z_k z]/2R_{kj} \quad (27)$$

$$\sqrt{(x_k - x)^2 + (y_k - y)^2 + (z_k - z)^2} = [R_{kl}^2 + x_k^2 - x_l^2 + y_k^2 - y_l^2 + z_k^2 - z_l^2 + 2x_l x - 2x_k x + 2y_l y - 2y_k y + 2z_l z - 2z_k z]/2R_{kl} \quad (28)$$

The equation set can now be simplified by substituting x_{ji} for $x_j - x_i$, y_{ji} for $y_j - y_i$ and so on.

$$\sqrt{(x_i - x)^2 + (y_i - y)^2 + (z_i - z)^2} = [R_{ij}^2 + x_i^2 - x_j^2 + y_i^2 - y_j^2 + z_i^2 - z_j^2 + 2x_{ji}x + 2y_{ji}y + 2z_{ji}z]/2R_{ij} \quad (29)$$

$$\sqrt{(x_i - x)^2 + (y_i - y)^2 + (z_i - z)^2}$$
$$= [R_{ik}^2 + x_i^2 - x_k^2 + y_i^2 - y_k^2 + z_i^2 - z_k^2 + 2x_{ki}x + 2y_{ki}y + 2z_{ki}z]/2R_{ik} \quad (30)$$

$$\sqrt{(x_k - x)^2 + (y_k - y)^2 + (z_k - z)^2}$$
$$= [R_{kj}^2 + x_k^2 - x_j^2 + y_k^2 - y_j^2 + z_k^2 - z_j^2 + 2x_{jk}x + 2y_{jk}y + 2z_{jk}z]/2R_{kj} \quad (31)$$

$$\sqrt{(x_k - x)^2 + (y_k - y)^2 + (z_k - z)^2}$$
$$= [R_{kl}^2 + x_k^2 - x_l^2 + y_k^2 - y_l^2 + z_k^2 - z_l^2 + 2x_{lk}x + 2y_{lk}y + 2z_{lk}z]/2R_{kl} \quad (32)$$

Equations (5)–(8) are now in a useful arrangement. Equations (29)–(32), when squared, are intersecting hyperboloids. By equating Eqs. (29) and (30) to form Eq. (33), we can derive a plane equation in the form of $y = Ax + By + C$ by rearranging the terms as shown in Eqs. (34) and (35).

$$[R_{ij}^2 + x_i^2 - x_j^2 + y_i^2 - y_j^2 + z_i^2 - z_j^2 + 2x_{ji}x + 2y_{ji}y + 2z_{ji}z]/2R_{ij}$$
$$= [R_{ik}^2 + x_i^2 - x_k^2 + y_i^2 - y_k^2 + z_i^2 - z_k^2 + 2x_{ki}x + 2y_{ki}y + 2z_{ki}z]/2R_{ik} \quad (33)$$

$$R_{ik}[R_{ij}^2 + x_i^2 - x_j^2 + y_i^2 - y_j^2 + z_i^2 - z_j^2]/2 - R_{ij}[R_{ik}^2 + x_i^2 - x_k^2 + y_i^2 - y_k^2 + z_i^2 - z_k^2]/2 = R_{ij}[x_{ki}x + y_{ki}y + z_{ki}z] - R_{ik}[x_{ji}x + y_{ji}y + z_{ji}z] \quad (34)$$

$$x[R_{ij}x_{ki} - R_{ik}x_{ji}] + y[R_{ij}y_{ki} - R_{ik}x_{ji}] + z[R_{ij}z_{ki} - R_{ik}z_{ji}]$$
$$= R_{ik}[R_{ij}^2 + x_i^2 - x_j^2 + y_i^2 - y_j^2 + z_i^2 - z_j^2]/2 - R_{ij}[R_{ik}^2 + x_i^2 - x_k^2 + y_i^2 - y_k^2 + z_i^2 - z_k^2]/2 \quad (35)$$

Equation (35) is now in the desired form of a plane equation as follows:

$$y = Ax + Bz + C \quad (36)$$

where

$$A = \left[\frac{R_{ik}x_{ji} - R_{ij}x_{ki}}{R_{ij}y_{ki} - R_{ik}y_{ji}}\right] \quad (37)$$

and

$$B = \left[\frac{R_{ik}z_{ji} - R_{ij}z_{ki}}{R_{ij}y_{ki} - R_{ik}y_{ji}}\right] \quad (38)$$

and

$$C = \frac{R_{ik}[R_{ij}^2 + x_i^2 - x_j^2 + y_i^2 - y_j^2 + z_i^2 - z_j^2] - R_{ij}[R_{ik}^2 + x_i^2 - x_k^2 + y_i^2 - y_k^2 + z_i^2 - z_k^2]}{2[R_{ij}y_{ki} - R_{ik}y_{ji}]} \quad (39)$$

Similarly, equating Eqs. (31) and (32) produces a second plane equation $y = Dx + Ey + F$. The resulting set of equations are:

$$y = Dx + Ez + F \quad (40)$$

where

$$D = \left[\frac{R_{kl}x_{jk} - R_{kj}x_{lk}}{R_{kj}y_{lk} - R_{kl}y_{jk}}\right] \quad (41)$$

and

$$E = \left[\frac{R_{kl}z_{jk} - R_{kj}z_{lk}}{R_{kj}y_{lk} - R_{kl}y_{jk}}\right] \quad (42)$$

and

$$F = \frac{R_{kl}[R_{kj}^2 + x_k^2 - x_j^2 + y_k^2 - y_j^2 + z_k^2 - z_j^2] - R_{kj}[R_{kl}^2 + x_k^2 - x_l^2 + y_k^2 - y_l^2 + z_k^2 - z_l^2]}{2[R_{kj}y_{lk} - R_{kl}y_{jk}]} \quad (43)$$

Equating the plane Eqs. (36) and (40) produces a linear equation for x in terms of z.

$$Ax + Bx + C = Dx + Ez + F \quad (44)$$

$$x = Gz + H \quad (45)$$

where

$$G = \frac{E - B}{A - D} \quad (46)$$

and

$$H = \frac{F - C}{A - D} \quad (47)$$

Substituting Eq. (45) back into Eq. (36) produces a linear equation for y in terms of z.

$$y = A(Gz + H) + Bz + C \quad (48)$$

$$y = Iz + J \quad (49)$$

where

$$I = AG + B \quad (50)$$

and

$$J = AH + C \quad (51)$$

Equations (45) and (49) are now substituted back into Eq. (30) to derive the position z.

$$2R_{ik}\sqrt{(x_i-(Gz+H))^2+(y_i-(Iz+J))^2+(z_i-z)^2} = [R_{ik}^2+x_i^2-x_k^2+y_i^2-y_k^2+z_i^2-z_k^2 + 2x_{ki}(Gz+H)+2y_{ki}(Iz+J)+2z_{ki}z] \quad (52)$$

$$2R_{ik}\sqrt{(G^2z^2-2Gz(x_i-H)+(x_i-H)^2)+(I^2z^2-2Iz(y_i-J)+(y_i-J)^2)+(z^2-2z_iz+z_i^2)} = Lz+K \quad (53)$$

where

$$K = R_{ik}^2+x_i^2-x_k^2+y_i^2-y_k^2+z_i^2-z_k^2+2x_{ki}H + 2y_{ki}J \quad (54)$$

and

$$L = 2[x_{ki}G+y_{ki}I+2z_{ki}] \quad (55)$$

$$4R_{ik}^2[G^2z^2+I^2z^2+z^2-2Gz(x_i-H)-2Iz(y_i-J) - 2z_iz+(x_i-H)^2+(y_i-J)^2+z_i^2] = L^2z^2+2KLz+K^2 \quad (56)$$

$$4R_{ik}^2[G^2+I^2+1]z^2-8R_{ik}^2[G(x_i-H)+I(y_i-J) + z_i]z+4R_{ik}^2[(x_i-H)^2+(y_i-J)^2+z_i^2] = L^2z^2+2KLz+K^2 \quad (57)$$

To obtain z, Eq. (57) is rearranged into a binomial equation.

$$Mz^2-Nz+O=0 \quad (58)$$

where

$$M = 4R_{ik}^2[G^2+I^2+1]-L^2 \quad (59)$$

and

$$N = 8R_{ik}^2[G(x_i-H)+I(y_i-J)+z_i]+2LK \quad (60)$$

and

$$O = 4R_{ik}^2[(x_i-H)^2+(y_i-J)^2+z_i^2]-K^2 \quad (61)$$

The solution for z is:

$$z = \frac{N}{2M} \pm \sqrt{\left(\frac{N}{2M}\right)^2-\frac{O}{M}} \quad (62)$$

The z coordinate can be put back into the linear Eqs. (45) and (49) to solve for the coordinates x and y.

VHDL MODEL

The equations for the x, y and z position of the mobile was modeled using VHDL. The numeric_std package was used to construct the VHDL model that was readily synthesized into a low power digital circuit. The details of the circuit are beyond the scope of this paper. The input signals of the model are the x, y, z positions of four GPS satellites i, j, k, l in meters, and the signal TOAs from the individual satellites to the mobile in nanoseconds. The input signal assignments are *xi*, *yi*, *zi*, *ti*, *xj*, *yj*, *zj*, *tj*, *xk*, *yk*, *zk*, *tk*, *xl*, *yl*, *zl* and *tl*.

GPS satellite altitudes are approximately 10,900 nautical miles (20,186,800 m). Therefore, the TOA range is roughly 6,700,000–7,600,000 ns. This means the input signals can be adequately described by a 32-bit vector. In order to perform signed arithmetic operations, the input signal assignments are of type SIGNED. The binary representation for negative numbers is 2's complement. The TDOAs are converted to distances by multiplying them by the binary representation of 100,000, and then dividing the result by the binary representation of 333,564 ns/m.

Since all signal and variable assignments are vectors representing integers, a method for maintaining adequate precision in divide and square root operations is needed. This will be achieved by multiplying the numerator by the binary representation of 1.0×10^{10} in divide operations. This method is preferred to using decimal point notation to decrease the complexity of the model. However, the length of the vectors increases for successive multiplication operations, leading to a 200-bit vector for the interim value O.

The numeric_std package does not contain an overloaded square root operator. Therefore, Dijkstra's bisection algorithm [10] is used to compute the integer square root of a positive integer represented by a 64-bit vector. Sixty four bits is deemed adequate since the position z and the square root term cannot be larger than 32 bits by definition.

The square root operation gives two values for z, so the output signals $z1$, $z2$, $x1$, $x2$, $y1$, $y2$ are for two possible mobile positions. The z value representing the mobile position can be determined by using a fifth satellite, or checking if the value is in the horizon of the four satellites relative to earth. The details of the VHDL model of the algorithm are provided in Appendix A.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Agilent Technolgies. "Cell Power, AWGN (Additive White Gaussian Noise) Power and Total RF Power." wireless.agilent.com. http://wireless.agilent.com/rfcomms/refdocs/1xevdo/1xevdo_gen_bse_pwr_lvl_parms.php, (accessed 30 July 2008).

Awele Ndili, Stanford University and Dr. Per Enge, Stanford University. "GPS Receiver Autonomous Interference Detection." http://waas.stanford.edu/~wwu/papers/gps/PDF/interfere_detect_ann98.pdf, (accessed April 1998).

Baijal, Rajat and Arora, Manoj. "GPS: A Military Perspective." GIS Development.net. http://www.gisdevelopment.net/technology/gps/techgp0048.htm, (accessed 11 July 2008).

Balaei, A. T., J. Barnes, and A. G. Dempster. "Characterization of Interference Effects on GPS Signal Carrier Phase Error." Melbourne, Australia: Spatial Science Institute, Proceedings of SSC 2005 Spatial Intelligence, Innovation, Praxis: The national biennial Conference of the Spatial Science Institute, September 2005, (accessed 4 August 2008).

Balaei, A. T., A. G. Dempster, and J. Barnes. *A Novel Approach in Detection and Characterization of CW Interference of GPS Signal using Receiver Estimation of C/No*. Position, Location, and Navigation Symposium, 2006 IEEE/ION2006.

Bastide, F., C. Macabiau, and E. Chatre. "GPS Interference Detection and Identification using Multicorrelator Receivers."Alexandria, 2001.

Bastide, F., Christophe Macabiau, and DM Akos. "Automatic Gain Control (AGC) as an Interference Assessment Tool." 2003.

Boggs, Matt and Kenea C. Maraffio. *Mitigation Paths for Free-Space Jamming*. China Lake, California: GPS/INS Systems Section, Naval Air Warfare Center Weapons Division (NAWCWPNS), , http://www.fas.org/spp/military/program/nav/gpsjam.pdf, (accessed 17 July 2008).

Brown, Alison, Dale Reynolds, Darren Roberts, and Steve Serie. "Jammer and Interference Location System - Design and Initial Test."Alexandria, 1999.

Bucher, Ralph and D. Misra. "A Synthesizable VHDL Model of the Exact Solution for Three-Dimensional Hyperbolic Positioning System." *VLSI Design* 15, no. 2 (3 October 2001) 507-520.

Coffey, Bill U.S. Army Space and Missile Defense Command (SMDC). *On Point Warrior Quotes-Master Copy (Slide 54 of Powerpoint Presentation)*2008 Mass E-Mail (accessed 13 July 2008).

Danish Audio Connect. "Leaded Resistor Equivalent Circuit Diagram." http://www.dact.com/html/leaded_resistors.html, (accessed 19 September 2008).

Depriest, Dale. "NMEA Data." http://www.gpsinformation.org/dale/nmea.htm, (accessed 19 September 2008).

Forssell, Borje and Olsen, Trond. "GPS world - jamming GPS." GPS World. http://www.gpsworld.com/gpsworld/content/printContentPopup.jsp?id=43432, (accessed 19 September 2008).

Green Bay Professional Packet Radio. "Microstripline Analysis & Design Results." http://my.athenet.net/~multiplx/cgi-bin/strip.cgi (accessed 19 September 2008).

———. "Noise Jammer for the L1 GPS Frequency (1575.42 MHz)." http://www.qsl.net/n9zia/, (accessed 19 September 2008).

Gromov, Konstantin. "GIDL - Generalized Interference Detection and Localization System."State Research Center of Russia Elektropribor, 2003.

Guerriero, Bob LTC, Tom LTC James, and Jim LTC Rozzi. "The future of Army Space Forces - a vision to optimize tactical and operational space support". *The Army Space Journal,*2007. 12, http://www.smdc-armyforces.army.mil/ASJ/Edition.asp?E=2, (accessed 13 July 2008).

Haseloff, Robert "Hawg". "JNWC-Navwar-Threat Overview Brief (Unclassified Portion) United States Army FA-40 Symposium." Colorado Springs, Colorado, Joint Navigation Warfare Center, 2-5 September 2008 (accessed 12 September 2008).

Hyten, John C. "Hyten GPS Operations Past Present Future Overview Presentation." Authorstream.com. http://www.authorstream.com/Presentation/Janelle-54303-hyten-GPS-OperationsPast-Present-Future-Overview-Mission-Past-1978-as-Education-ppt-powerpoint/, (accessed 11 July 2008).

Jacqueline Bickerstaff. "The enemy inside GPS jammed by room, Host, Self." http://findarticles.com/p/articles/mi_m0BPW/is_3_16/ai_n13487592, (accessed 13 August 2008).

Jeffries, David. "What is Microstrip Transmission Line?" http://personal.ee.surrey.ac.uk/Personal/D.Jefferies/mstrip.html, (accessed 19 September 2008).

Joe Mehaffey. "Rain, Snow, Clouds and GPS Reception." http://www.gpsinformation.net/gpsclouds.htm, (accessed 14 August 2008).

Krasner, Norman F. *Reducing Cross-Interference in a Combined GPS Receiver and Communication System*, Edited by 09/874747.

Lazar, Steven. *Method for Detecting and Locating Sources of Communication Signal Interference Employing both a Directional and an Omni Antenna*, Edited by 08/766723.

Lin, David M., James B. Y. Tsui, and Dana Howell. "Direct P(Y)-Code Acquisition Algorithm for Software GPS Receivers."Alexandria, 1999.

Lt. Trond Birger Olsen and Dr. Borje Forssell. "Jamming GPS susceptibility of some civil GPS receivers." http://www.avweb.com/news/avionics/182754-1.html, (accessed 8 July 2008).

Miller, LE. http://w3.antd.nist.gov/wctg/manet/docs/uwbgpsprop.pdf (accessed 14 August 2008).

Navtech GPS. "GNSS Facts." Navtech GPS. http://www.navtechgps.com/extra/GNSSfacts.asp (accessed 14 August 2008).

Navtech GPS. “GPS L1 Link Budget.” http://www.navtechgps.com/pdf/GPS L1 Link Budget ERP.pdf, (accessed 22 September 2008).

Navtech GPS. “GPS L2 Link Budget.” http://www.navtechgps.com/pdfGpsNetworking_LinkBudget.pdf, (accessed 22 September 2008)

Oshman, Y. and M. Koifman. "Robust, IMM-Based, Tightly-Coupled INS/GPS in the Presence of Spoofing [Interacting Multiple Model]."American Institute of Aeronautics and Astronautics, 2004.

Oshman, Yaakov and Mark Koifman. "Robust navigation using the Global Positioning System in the presence of spoofing." 29, No. 1 (Journal of Guidance, Control, and Dynamics. Vol. 29, No. 1, January-February, 2006): 95-104.

Rockwell International. "GPS Jamming." Rockwell International. http://www.ac11.org/gps1.htm, (accessed 10 September 2008).

Rog, Andrey L. *Multiple-Channel Digital Receiver for Global Positioning System*, Edited by 09/508936.

United States Coast Guard. "Global Positioning System Standard Positioning Service Signal Specification, 2nd Edition." USCG. http://www.navcen.uscg.gov/pubs/gps/sigspec/gpssps1.pdf, (accessed 14 August 2008).

United States Coast Guard. "Global Positioning Service Standard Positioning Service Signal Specification Annex A, Standard Positioning Service Performance Specification." USCG. http://www.navcen.uscg.gov/pubs/gps/sigspec/gpsspsa.pdf, (accessed 14 August 2008).

United States Naval Observatory. "USNO NAVSTAR Global Positioning System." http://tycho.usno.navy.mil/gpsinfo.html, (accessed 19 September 2008).

White, Nathan A., Peter S. Maybeck, and Stewart DeVilbiss. "Detection of interference/jamming and spoofing in a DGPS-aided inertial system." *IEEE Transactions on Aerospace and Electronic Systems* 34, No. 4 (IEEE Transactions on Aerospace and Electronic Systems. Vol. 34, No. 4, 1208-1217. October 1998): 1208-1217.

Wikipedia contributors. "Aviaconversiya." Wikipedia, The Free Encyclopedia. http://it.wikipedia.org/wiki/aviaconversiya?oldid=17841971, (accessed 19 September 2008).

———. "Multilateration." Wikipedia, The Free Encyclopedia. http://en.wikipedia.org/wiki/multilateration?oldid=228786716, (accessed 6 August 2008).

Winer, Bette M., Paul Manning, E. M. Geyer, Joseph Ruggiero, and Philip McCarty. "GPS Interference Source Location and Avoidance Systems."Alexandria, 1997.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Larry Mize
   Army Space and Missile Defense Command
   Future Warfare Centere, Directorate of Combat Developments
   Chief of Training
   Colorado Springs, Colorado

4. LTC Bob Guerriero
   Chief, Capabilities Integration Division
   Future Warfare Center SMDC/ARSTRAT
   Huntsville, Alabama

5. Robert “Hawg” Haseloff
   Senior Operations Analyst
   Joint Navigation Warfare Center
   Kirtland AFB, New Mexico