15400 Calhoun Drive, Suite 400
Rockville, Maryland, 20855
(301) 294-5200
http://www.i-a-i.com

Intelligent Automation Incorporated

UWB Enhanced Time Difference of Arrival System

Final Report

Reporting Period: 10/1/2009 – 6/30/2012

Contract No. # 2007-RG-CX-K179
Sponsored by: National Institute of Justice

COTR/TPOC: Dr. Frances Scott, Frances.Scott@usdoj.gov
(202) 305-9950

Prepared by

Benjamin Lonske
Eric van Doorn
Satya Ponnaluri
Arvind Bhat

This project was supported by Award No. 2007-RG-CX-K179 awarded by the National Institute of Justice, Office of Justice Programs, U.S. Department of Justice. The opinions, findings, and conclusions or recommendations expressed in this publication/program/exhibition are those of the author(s) and do not necessarily reflect those of the Department of Justice.

Final Report – UWB Enhanced TDOA system
Submitted in accordance with requirements of NIJ Grant 2007-RG-CX-K179

Contents

1. Introduction

1. Meetings

A meeting was held with the COTR Dr. Frances Scott at the start of this phase of the project on June 28th 2010. IAI team presented the technical updates with a demonstration of the system result from Phase I and discussed the objects for Phase II. The TPOC found everything in order and requested some additional documents that were be provided by the IAI Contracts/Finance Departments. Since then, we have discussed progress with the COTR over the phone several times.

During the early part of the project, we had multiple phone conversations and a face to face meeting with Carl Finney of DRS-Technologies to discuss use of their cell phone receiver hardware for the project. Initially, it appeared that DRS Technologies had an interest in collaborating with us, with the objective of investigating or developing a civilian application for their cell phone locator technology. However, after several discussions it was determined that the DRS hardware was too expensive (>$20,000/node) to be practical for the application of locating cell phones in prisons, and that DRS Technologies did not want to make hardware available at lower cost to the project.

2. Prison Test

During the first year of the project, a channel sounding test was performed at a prison. The goal of the test was to carry out channel sounding measurements across

US's three popular cell phone frequency bands (GSM, WCDMA, PCS). The design of experiments was carried out based on physical layer features, in particular transmit bandwidth, frame format, modulation scheme and camp-on procedure, of three important cellular bands; GSM-850/1900, IS-95, and W-CDMA. A review study was made of these three bands; this was included as an Appendix in Progress Report #1 and will not be repeated here.

A review of the prison test is as follows:

Equipment Used

- HP 8594E Spectrum Analyzer (2)
- HP 8648C Signal Generator (1)
- Tri-Band Antennas (3)
- Power Amplifiers (2)

Software/Scripts Used

A transmitter script was developed using Labview 8.2. The script, which was used to program the HP 8648C Signal Generator, allowed the user to specify the start and stop frequency, step size, the signal amplitude as well as the seconds to wait between switching from one frequency to another (minimum 0.15 sec). The script also provided the user the capability to define the number of frequency sweeps to be carried out.

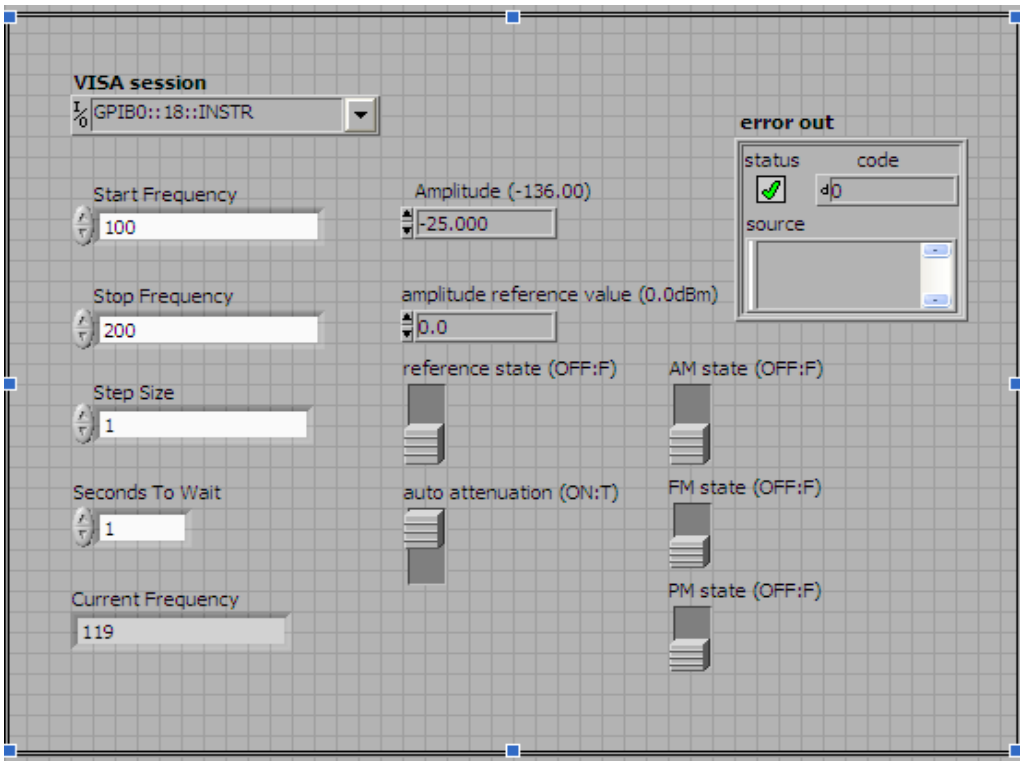


Figure 1: Screenshot of the TX Labview script GUI

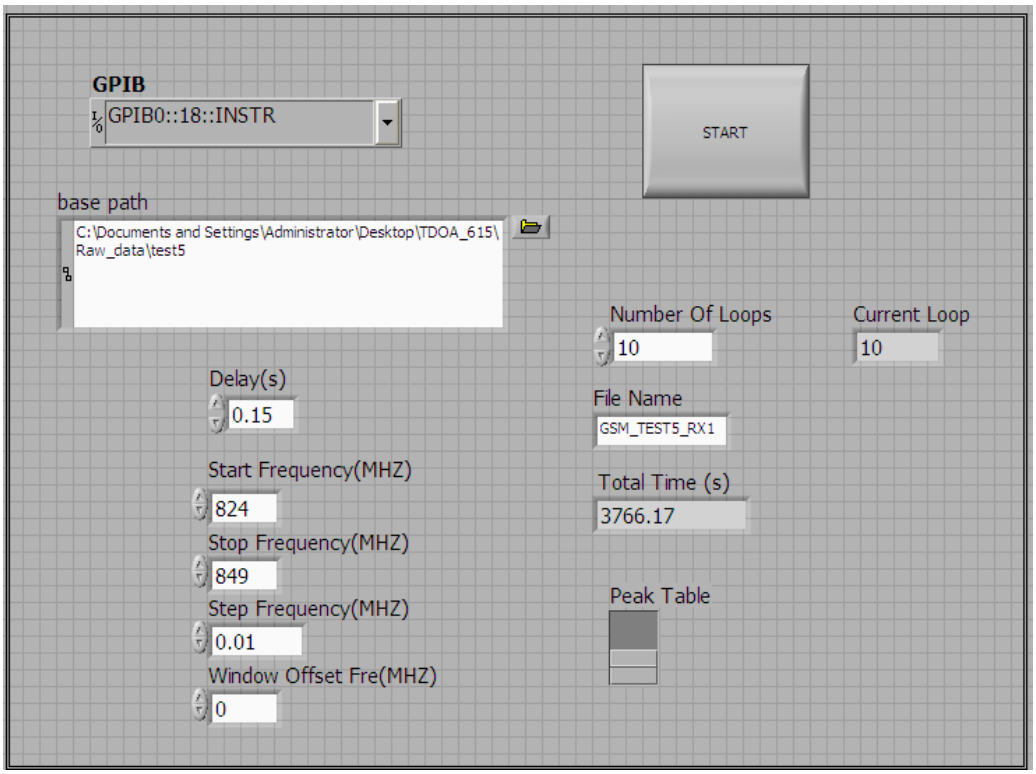


Figure 2: Screenshot of the RX Labview script GUI

A receiver script was also developed using Labview 8.2. The script, which was used to program the two HP 8594E Spectrum Analyzers, allowed the user to specify the start and stop frequency, step size as well as the seconds to wait between switching from one frequency to another. The spectrum analyzer recorded the raw amplitude data to a text files. The folder path where these text files should be saved could be specified in the 'Base Path' box and the name of the text file can be specified in the 'File Name' box.

Frequency Bands

The following bands were covered during the prison tests:

- GSM: 824 to 849 MHz with 200 KHz step size
- WCDMA: 1710 to 1755 MHz with 200 KHz step size
- PCS: 1850 to 1910 MHz with 200 KHz step size

The transmitted power for all bands across all tests was 24 dBm.

Description of test set-up

Laptops running the Labview scripts connected to the signal generator/spectrum analyzers through the GPIB cable. The output of the signal generator is connected to a power amplifier (40 dB gain for GSM band, 26.5 dB gain for WCDMA and PCS bands). The tri-band antenna is connected to the output of the power amplifier. On the RX side, the tri-band antenna is connected to the signal input of the spectrum analyzer.

Description of test run

For each TX location, three tests were performed; one for each of the cell phone frequency bands i.e. GSM, WCDMA and PCS. Using push to talk radios, the user assigned to each test set-up synchronizes the start of the test readings for TX, RX1 and RX2. The number of frequency sweeps was set to ten for tests 1 through 18 and five for tests 19 through 24. The spectrum analyzer reference level was set at -10 dB. Each test run took about 3-5 minutes to complete the specified number of frequency sweeps. The antenna for RX1 was propped up on a 6 ft. pole.

Location of test set-up

The image in Figure 3 shows the section of the Lawrenceville Correctional Facility prison where the tests were performed. The below key shows the specific test locations.

RX2A - Location of RX2 for Tests 1 through 21
RX2B - Location of RX2 for Tests 22 through 24.
TXA – Location of TX for Tests 1, 2, 3 performed at bottom level
TXA – Location of TX for Tests 10, 11, 12 performed at upper level
TXB – Location of TX for Tests 4, 5, 6 performed at bottom level
TXB – Location of TX for Tests 13, 14, 15 performed at upper level
TXC – Location of TX for Tests 7, 8, 9 performed at bottom level
TXC – Location of TX for Tests 16, 17, 18 performed at upper level

TXD – Location of TX for Tests 19 through 24 performed at upper level

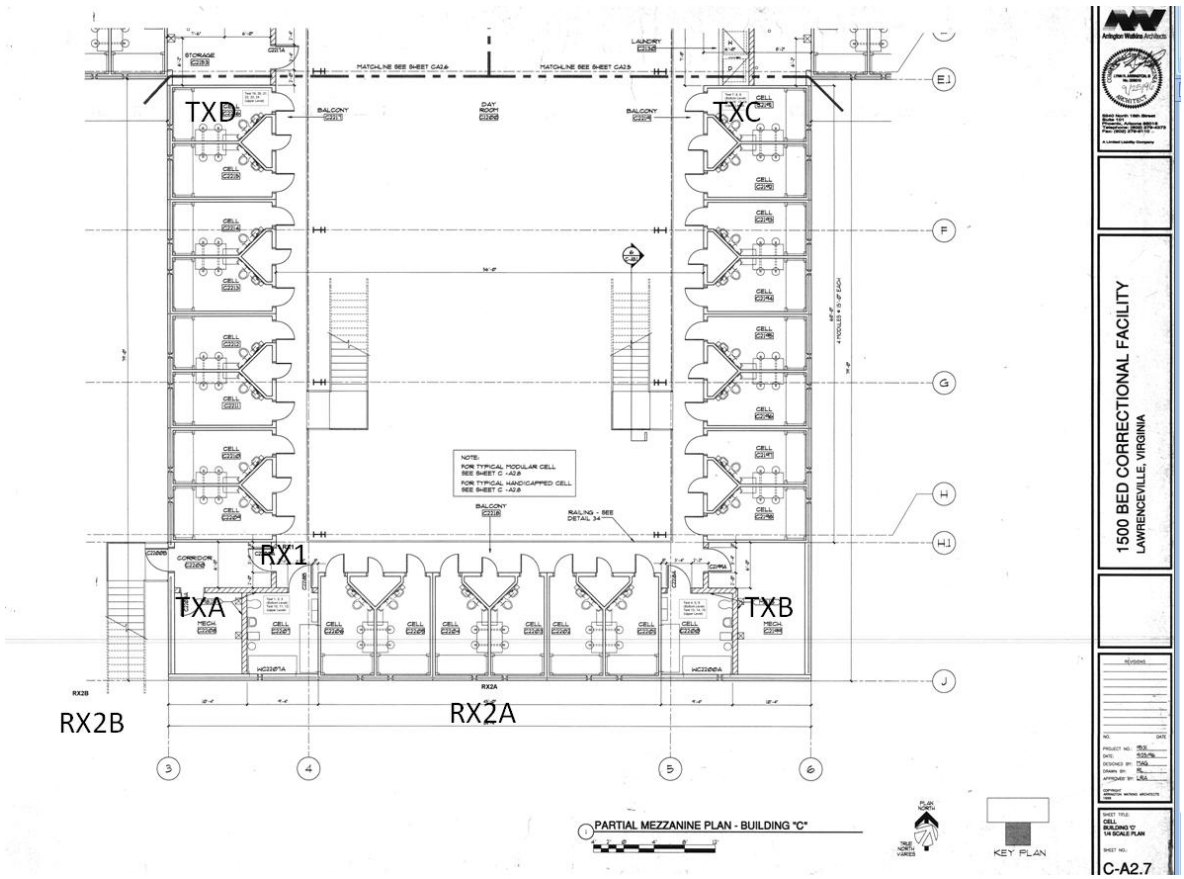


Figure 3: Layout of the prison building where the tests were carried out

Post processing script was developed using Matlab 7. The data captured by the spectrum analyzer and stored in the text files was the raw amplitude data i.e. the binary data stored as a bunch of arrays. The Matlab script took this raw data and using a predefined set of calculations, scaled the data to provide the actual amplitude readings in dB. From this, the max or mean amplitude points could be determined and plotted across the frequency band to see how they trended over the frequency sweep. An example plot is shown in Figure 4.

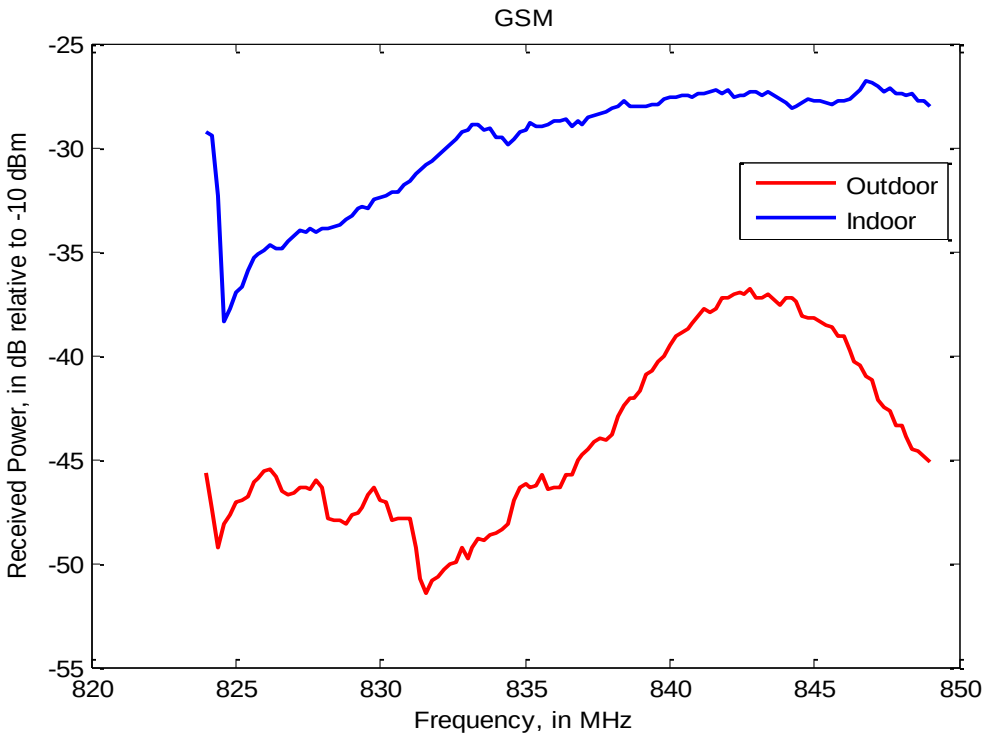


Figure 4: Max amp plot across the GSM band for RX1 (indoor) and RX2 (outdoor)

Results

Following are the key conclusions that can be drawn about the tests:

- The results indicate, as expected, that the signal received outside can be better than that received inside depending on the proximity of transmitter and receiver.
- High frequency signals (i.e., WCDMA 1710-1755 MHz and PCS 1850-1910 MHz) attenuate more than low frequency signals such as those of GSM 824-849 MHz.
- When the receiver and transmitter are far apart as is the case in the outdoor test scenarios corresponding to Test# {7,8,9}; {16,17,18}; {19,20,21}, the received signal is very weak, and the corresponding WCDMA and PCS signals are not captured by the Spectrum Analyzer.
- We observe significant frequency selective behavior in some test scenarios, especially for WCDMA and PCS signals, in both indoor and outdoor settings.

3. Initial System Design

During the Summer and Fall 2010 we performed extensive experiments on indoor localization of RF emitters for this project and also under the DARPA's LANDroids program. The majority of the experiments were to determine the accuracy of Round-Trip-Time of Flight (RTOF) ranging using 900MHz signals with a few MHz of bandwidth. These signals are very similar to those used in CDMA2000, and the experiments clearly demonstrated, as expected, that multipath significantly affects RTOF ranging, and hence

TDOA-based localization. For location of a *mobile* emitter, movement of the receiver or transmitter and/or using redundant receivers allows averaging out of these multipath errors, and we found that we could locate our emitters (which had several MHz of bandwidth) with several feet accuracy when emitters moved over several feet, and 5 or 6 reference emitters and know location were used for triangulation. For the current project, the emitter will be largely stationary, and we expect to combat multipath error by use of multiple receivers and by extensive "fingerprinting" calibration. By this, we mean moving a cell phone from cell to cell, and recording the TDOA measurements in each reference receivers for each cell phone location.

These experimental results, along with the unavailability of the DRS technologies hardware, motivated the development of hardware that have the potential to be produced at relatively low cost (a few hundred dollars per node), and that would require minimal installation so that a larger number of nodes can be practically accommodated. This hardware was foreseen as being must able to detect and record cell phone signals, be synchronized to ~ns accuracy, and transfer data wirelessly between them. The details of this system design are shown below.

System Architecture

We envisioned a Master-Slave architecture for the location of cell phones by means of TDOA (Figure 5).

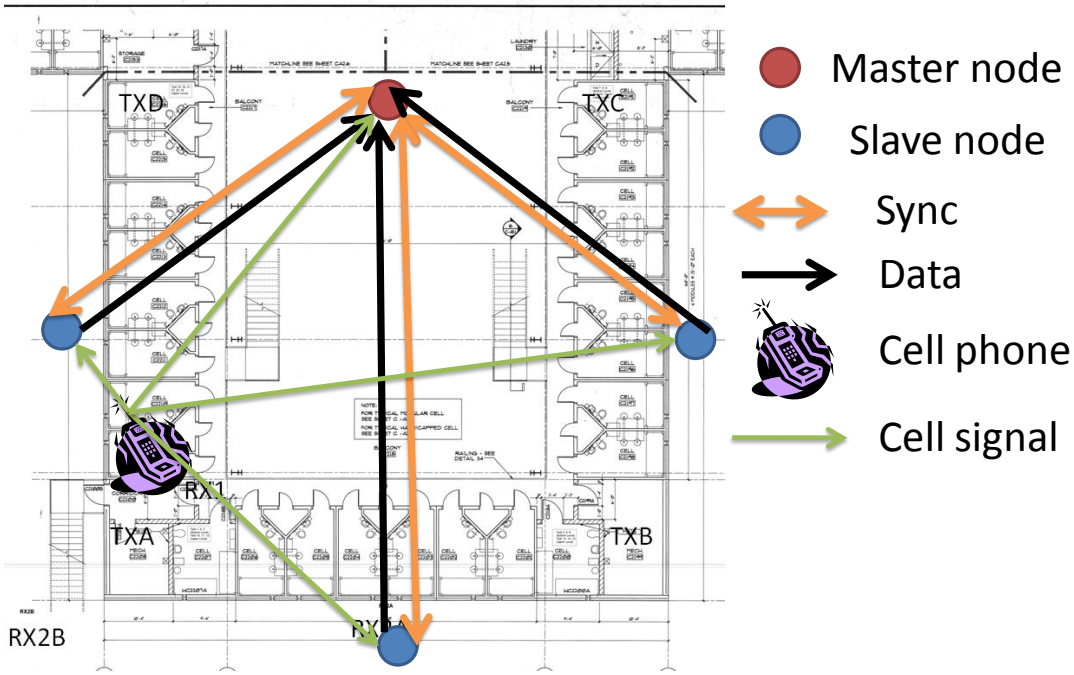


Figure 5. Master-SlaveTDOA Architecture

The architecture consists of Master and Slave transceivers. Each transceiver is capable of receiving cell phone signals, and exchange sync signals and data. Each node will act as a state machine enabling independent cell phone activity, and signal recording. After each detection; synchronization is initialized by the Master and sync signals are exchanged

round-robin fashion with the Slaves. After syncing, each Slave transmits RF and TOA data to the Master. The Master transfers data to a PC, which performs the TDOA calculation, and displays the results. A flow diagram of the Master and Slave state machines is shown in Figure 6.

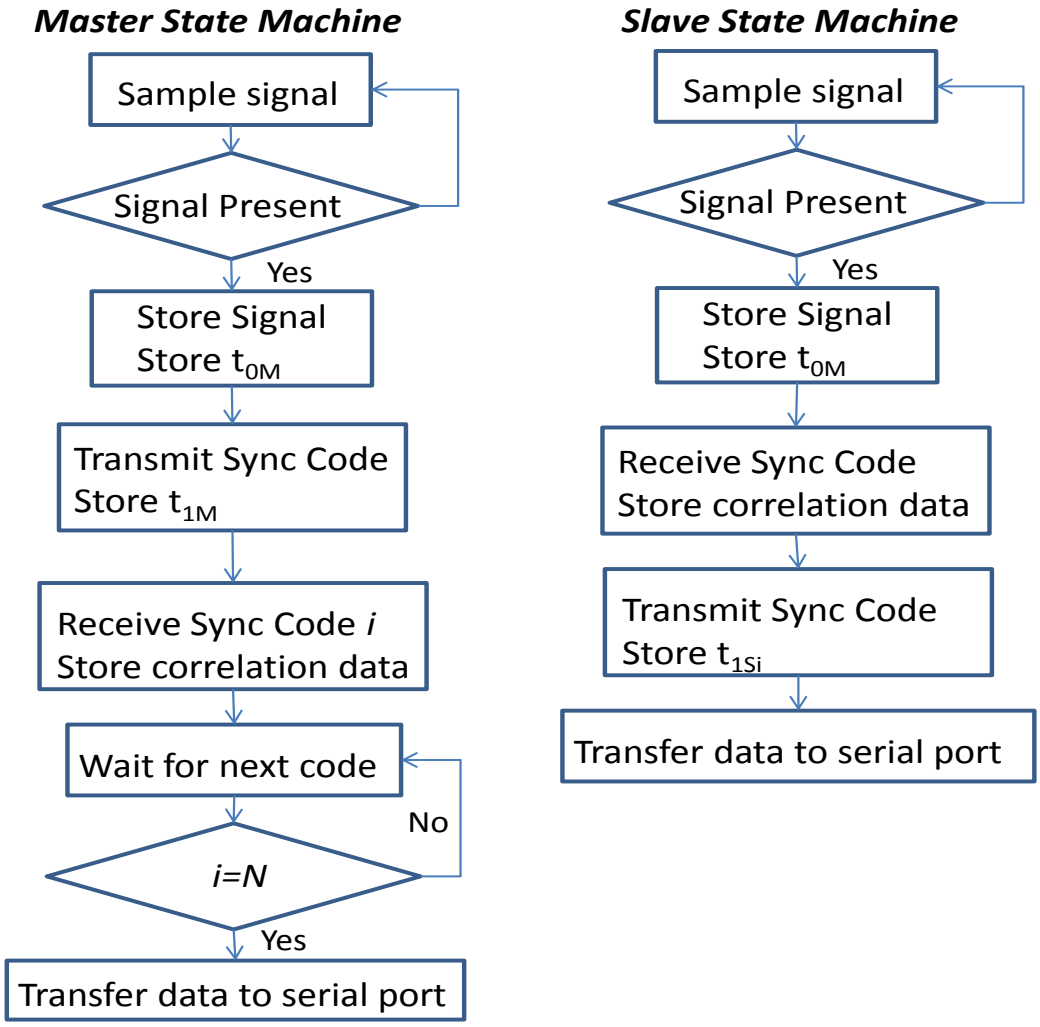


Figure 6. Master and Slave node state machines.

3.1. Hardware Design

The design of our initially in-house designed cell phone receiver board is shown below, in Figure 7.

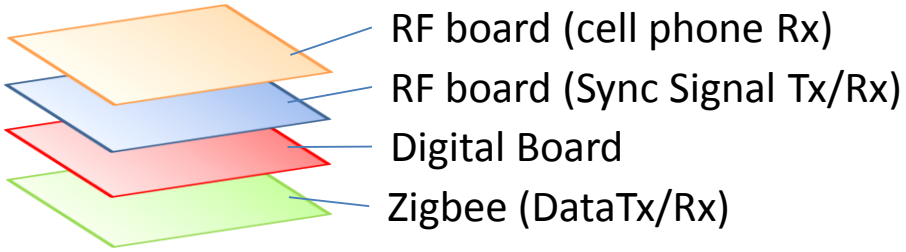


Figure 7. Hardware Node board-level design

The hardware consisted of four boards per node: 1) an RF receive board for receiving the cell phone signal, in the current hardware it will be tuned to the 850 GSM only, 2) a Sync RF board transmit receive board used to transmit and receive synchronization signals, tuned to the 900MHz band, 3) a digital board used to digitize and store received (base-band) signals, and generate sync signals, and 4) a COTS Zigbee board used to transfer data between the nodes. Of these 4 boards, the bottom 3 have been build/bought and integrated in to a single node.

Synchronization

The Sync RF board is used to transmit and receive sync signals. It interfaces to the digital board. It is capable of receiving and transmitting RF signals between 800MHz and 2.7GHz. Synchronization is achieved by exchanging coded signals between Master and Slave nodes. Each code is 64 bits long, we use BPSK modulation and pulse shaping to limit the bandwidth to within the 28MHz allowed in the unlicensed FCC 900MHz band. In the receiver, the signal is down–converted, sampled, and correlated with a template code. When the received samples and the template code 'line up', the time-of-arrival of the signal is determined.

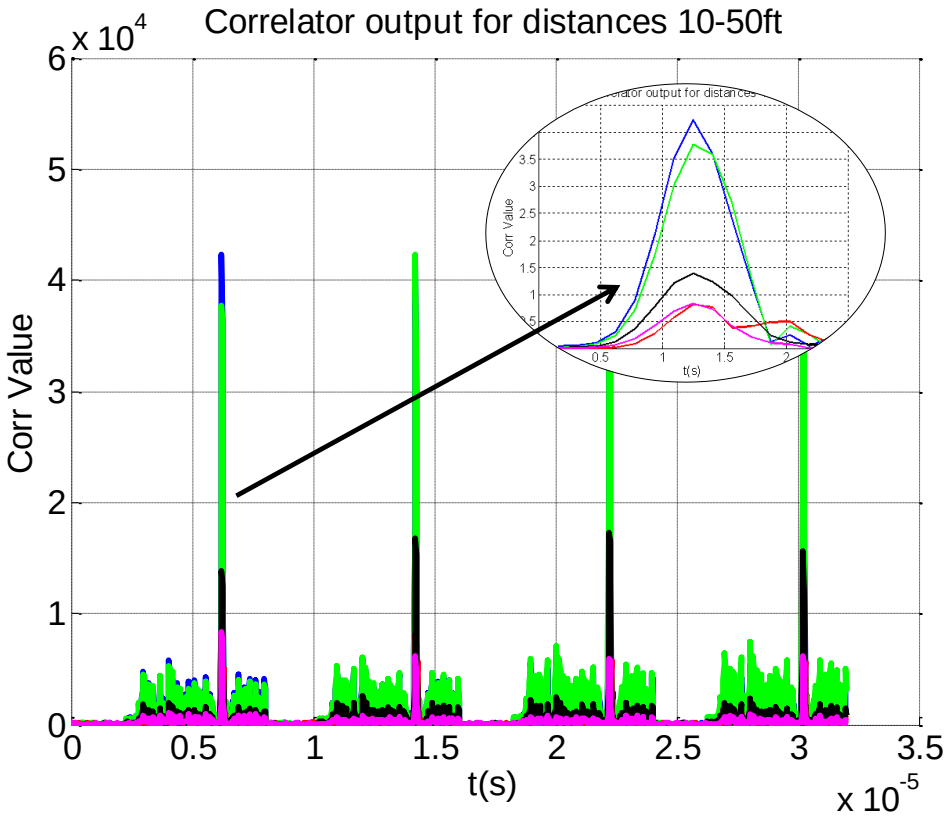


Figure 8. Correlator value as function of time. Codes are sent repeatedly. Time of arrival is estimated to within 1 sample time (1/64e6Hz) or 16ns.

After the time of arrival is computed, the Slave transmits a code back to the Master, it computes the corresponding time of arrival. After subtraction of (constant) hardware delays due to propagation through the analog frontend, the time of arrival values are used to compute the clock offset between Master and Slave. Currently, the synchronization accuracy is 16ns, we detail our approach to reaching ~1-2ns accuracy (needed for ~1-2ft accuracy localization) below.

Cell phone receiver board

The top receiver front end board (Figure 9), used to receive cell phone signals is very similar to the second board. The current design would allow detection of any single cell phone band by replacement of a filter, and a small firmware change to tune the local oscillator to the center of the band. The currently planned design would allow detection and localization of phones in one of the four bands in use in the US.

Figure 9. Cell phone receiver PCB.

Integration

We have interfaced the RF frontend to the digital board, and were able to successfully digitize samples for a test tone (Figure 10).

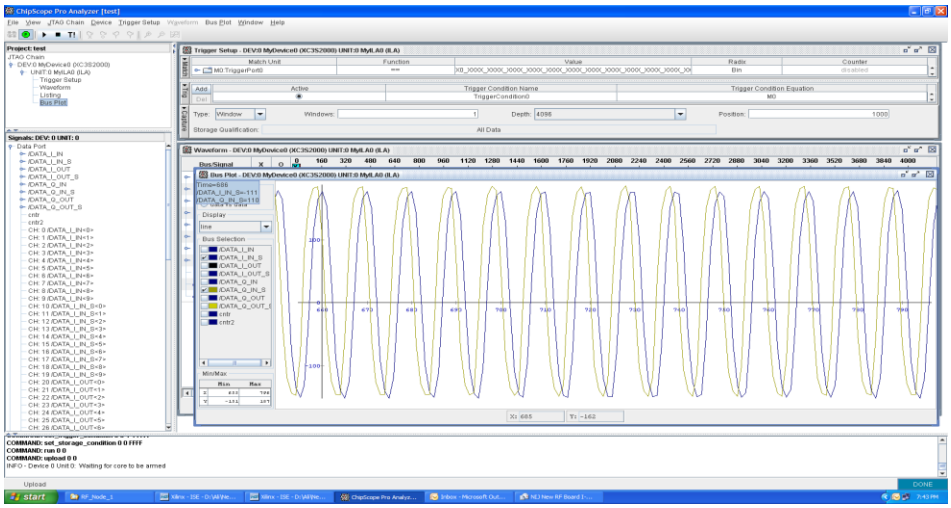


Figure 10. Received digital samples.

The current prototype works for two of the three bands. We have tested the RF frontend, and its performance is consisted with receiving two cell phone signals in the 830MHz and 1900MHz bands. We show test results for the RF frontend in Figure 11. WE show the received power vs. Frequency as measured with the vector analyzer. The two cell phone pass bands are clearly visible. The board will be extended to the third band under the current work. Multiple units are now being fabricated.

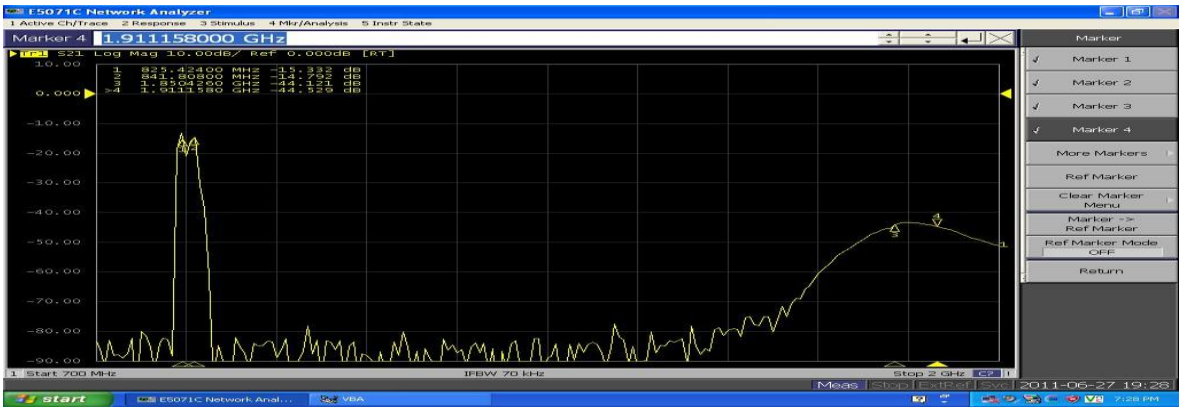


Figure 11. RF front-end results for 830MHz band and 1900MHz band

Communication

The design was to use COTS Zigbee radios to communicate between nodes. The radio interfaces to the digital board using a serial port. Data rates of up to 100Kbs can be achieved, allowing for data transfer of received RF signals within a fraction of a second.

Synchronization hardware

We completed the hardware for initial synchronization (Figure 12, left), and have run tests to determine its accuracy. We conducted tests to measure the received SNR of our synchronization approach. In order to measure the SNR, we transmit a code of length 64 bits, at a rate of 15 Mbps, and measure the correlation performance. The transmitter and receiver are connected using a cable with an attenuator of 24 dB. The transmitted power is around 26 dBm, so that the received power is around 2 dBm. The correlation plot is shown in the figure below. The peak value of the correlation is a measure of the received signal energy. In order to measure the noise power, we sample the output of A/D in the absence of any input, and the variance of the received samples is indicative of the noise variance. The ratio of signal energy and the noise variance is a measure of SNR. Based on the received SNR, it is possible to estimate the error in measurement of one way time of flight using the following equation[1]:

$$\sigma_\tau \leq \frac{T_b}{2}\sqrt{\left(\frac{d}{SNR}\right)}$$

Where we assume the receiver utilizes early-late correlation approach to estimate the time of arrival, with d denoting the correlation spacing between early and prompt correlation samples. If we assume a correlator spacing of 1 bit, then the performance is given by:

[1] P. Misra and P. Enge, *Global Positioning Systems: Signal, Measurements and Performance,* Second Edition. Ganga-Jamuna Press. 2006.

$$\sigma_\tau \leq \frac{T_b}{2}\sqrt{\frac{1}{SNR}}$$

Our initial measurements indicate a received SNR of 50 dB after correlation when transmitting a Gold code of length 64 at 15 Mbps, so that the expected error in time of arrival measurement is around 0.1 ns *for the wired case*.

In order to predict the performance *under wireless conditions*, we consider the following propagation path loss model (ITU indoor path loss model):

$$PL(d)_{dB} = 20\log f_{MHz} + 10n\log d + P - 28$$

where P denotes penetration factor for walls, n denotes the path loss exponent. Assuming $n = 3.3$, and 15 dB loss due to penetration at a frequency of 900 MHz, we obtain the path loss as follows:

$$PL(d)_{dB} = 46 + 33\log d$$

At a **distance of 1 m**, the path loss is therefore around 46 dB, resulting in a **received SNR of around 28 dB**, and the corresponding **time-of-arrival error is around 1.3 ns**.

In conclusion, we found that the received SNR or the correlation function (Figure 12, right) even at just a few meters of separation is too low to get sufficient accuracy for wireless operation. Hence, we have decided that to get sufficient accuracy ~1ns, the units have to be connected with cables. For the cabled case, the error will be well under 1ns for tens of meters of separation.

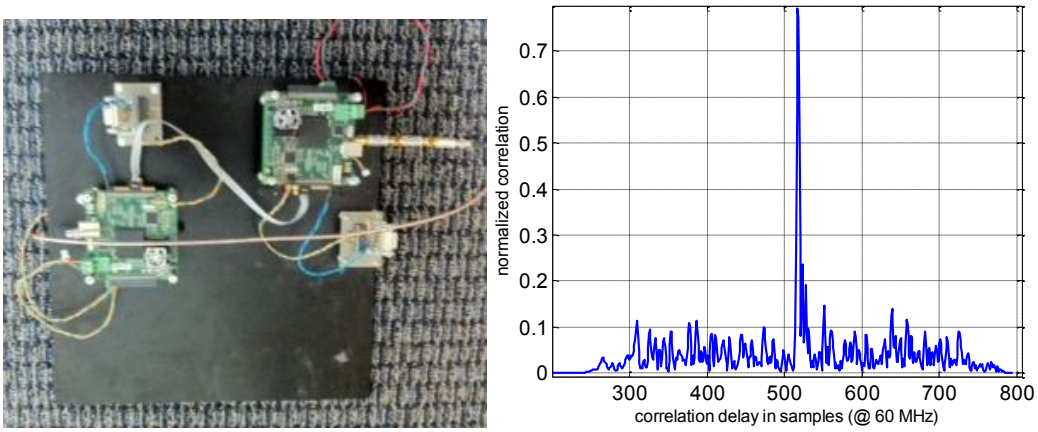


Figure 12. Synchronization hardware tested with cable connection, and correlation function.

2. Update on Cell Phone Tracking in Prisons

In the second year of the project, we examined the current state of the art in cell phone tracking was examined to see how IAI's system can best complement these approaches. There is a lot of excitement right now about managed access. This is the system where a multi-standard/multi-frequency cell phone base station is installed on prison grounds. Its objective is to draw all cell phones in the facility to connect to it. The managed access system has a list of approved cell phone phones (those of the warden, guards, etc.). The system allows these approved cell phones to place and receive calls, while all others are

dropped. Managed access has generated excitement because it is the first system that has been shown to sharply reduce contraband cell phone use in prisons, though this evidence has so far been limited to two pilot studies.

Managed access is a not a solution for every jail and prison, for several reasons. The first is it is expensive to install (~$1M) and therefore not practical for small facilities. The cost becomes even higher if an already existing high power base stations near the prison needs to be relocated due to the fact that it that might draw calls the managed access base station needs to catch. Second, the performance of managed access is necessarily compromised when used in prisons in urban areas, or in prisons that directly border residential or business areas. This is because the boundaries of the managed access "RF net" are not sharp and thus need to be pulled in from the perimeter of the grounds in the above cases so as to not effectively jam non-prison cell phones. The effect of this is to leave an unsecure border near the edge of the perimeter that can be exploited by inmates. Last, managed access blocks but does not locate cell phones. This allows for accessories such as cell phone cameras to be used, and also deprives prison personnel of useful forensic evidence gleamed by confiscating the cell phones.

The cell phone tracking system IAI is designing can complement managed access by locating the phones that try to make calls. It can also be used stand-alone in case where managed access is impractical.

3. Revised System Design for a Wired System

The original system, described above, was based around a system based on multiple receiver nodes that were to be synchronized either with wires or wirelessly. During the second year of the project, it was determined that this type of system would be difficult to synchronize to the necessarily degree of about 1nsec. Therefore, the system design was migrated to one in which there is one receiver/processor with four antenna ports. Long cables, each >100ft, extend from the receive ports to antennas located at the corners of a prison facility building. Since the same hardware is used to sample all four channels, synchronization is no longer an issue after calibrating for small differences in cable length.

3.1. Cell Phone Receiving Hardware

Cell phone signal receiving hardware based on the revised system design was built and tested. This hardware was based on that previously designed for an ongoing IAI project "Software Defined, Reconfigurable, Plug-and-Play Transceiver" for AFRL, Contract #. FA8650-10-C-1737. Details of the hardware will be described in the next progress report. In summary, there are four receive channels that can each sample at up to 400Msps. It has a direct conversion receiver that can sample signals at a higher bandwidth than the sampling rate via the use of aliasing and bandpass filtering. The processor used is Virtex-5 FPGA. Data is sent up to a PC running Matlab via Gigabit Ethernet.

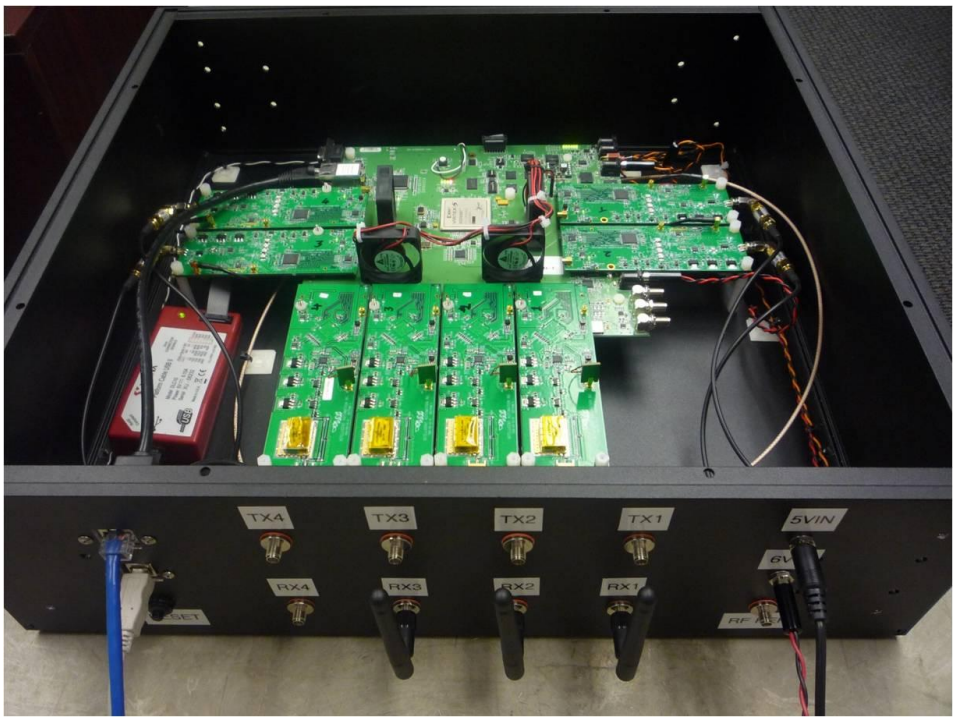


Figure 13: The 4-channel receive with the enclosure. Each of the four receive channels can be sampled at up to 400Msps. All RF, Power and User interfaces are available on the front-panel. The system communicates with a PC via a Gigabit Ethernet interface.

4. Matlab Data Analysis and Simulation Code

While the hardware was being designed and built, Matlab code was written to: a) simulate delayed CDMA2000 cell phone signals, b) input data over Ethernet from the receiving hardware, and c) analyze either the simulated or actual data to determine time differences between channels and location of the cell phone.

4.1. Simulation of CDMA2000 transmission

The method used to generate signals similar to those received from the receiving hardware is as follows (see Table 1). First, 100msecs worth of CDMA2000 baseband signal extracted from an existing Simulink simulation and was recorded in a .mat file. This baseband signal was sampled at 4.9152MHz, or four times the CDMA2000 baseband frequency of 1.2288MHz. We decimated this by two for a sampling frequency of 2.4576MHz, to better match what is received from the hardware. The signal was then re-sampled to 1GHz to allow for fine shifting of the signals. Signals from each of four simulated antenna are created, each with a different delay. From here, the signals from each antenna are resampled again, this time down to our actual hardware sampling rate of 62.5MHz (note the hardware actually samples at 250MHz for this system, but decimates by four to allow for more data to be stored). The baseband signals are then upconverted to the desired cell phone channel frequency. At this point, different channels models can be applied. We have so far tested with additive white Gaussian noise. In the next performance period, we will test with indoor channel models that include multipath effects.

Table 1: Simulation of cell phone signals

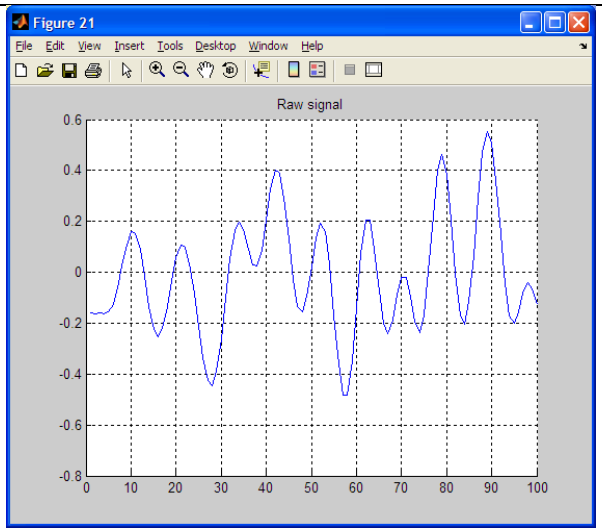


Figure 14: Cell phone baseband signal

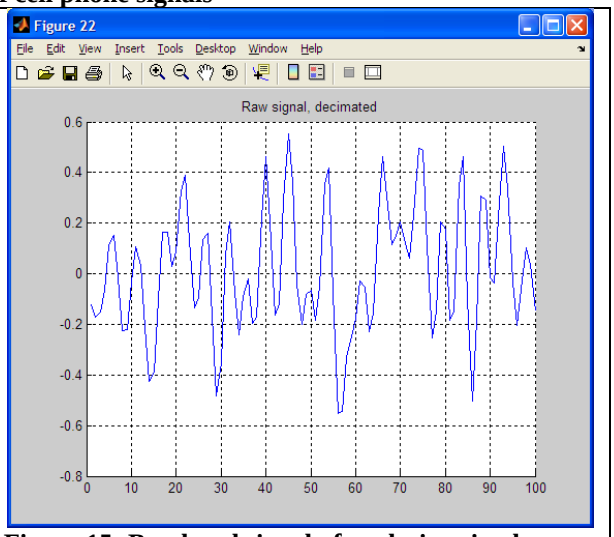


Figure 15: Baseband signal after decimating by two

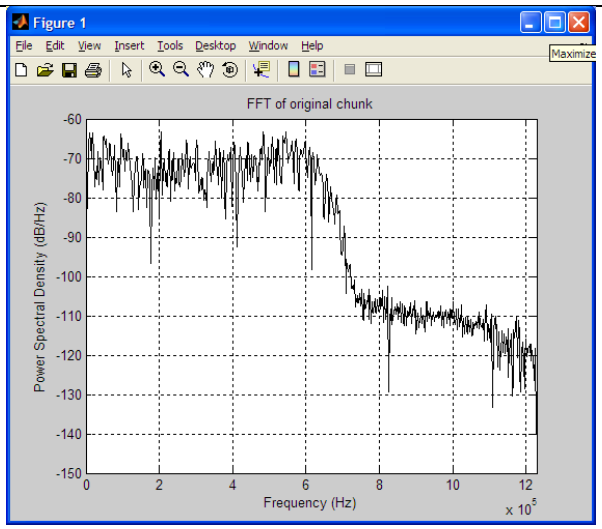


Figure 16: Spectrum of baseband signal showing a bandwidth of 1.2288MHz.

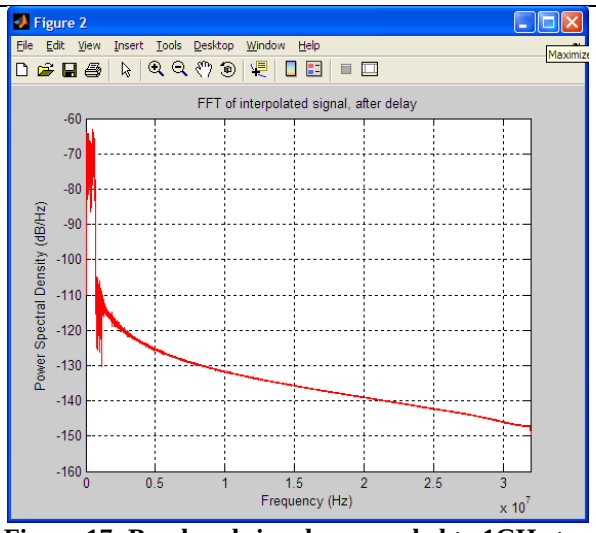


Figure 17: Baseband signal re-sampled to 1GHz to simulate delays with 1nsec increments.

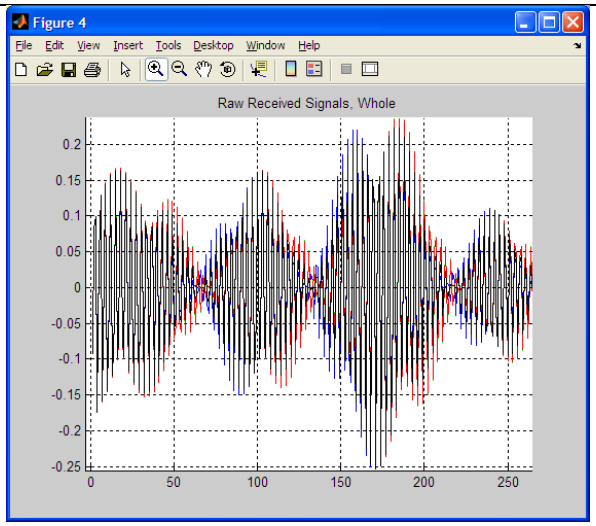


Figure 18: Resulting four delayed signals in time domain, after delays and upconverting to desired cell phone channel.

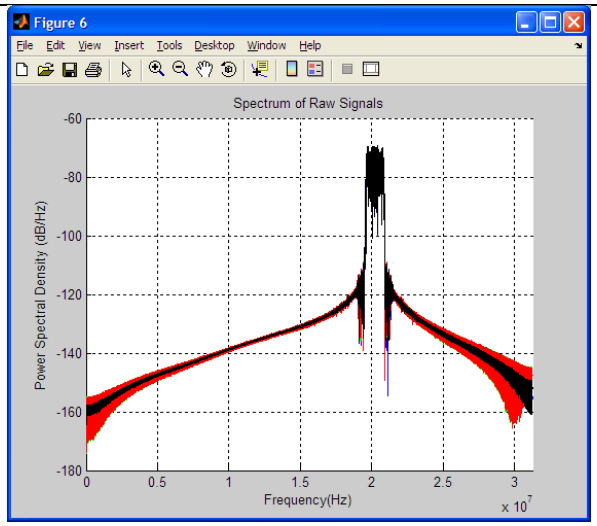


Figure 19: Spectrum of four signals after delaying and upconverting. Actual cell phone channel here is the shown 20MHz+71.7MHz+750MHz = 841.7MHz

5. Determining time difference and cell phone location

5.1. Determination of time difference between received signals

The following method is used to determine the time difference between each pair of antennas (see Table 2). First, the received signals are correlated. It is difficult to find an accurate peak of this signal from this correlation because it is both signal and negative and is not yet downconverted. Downconversion is not used because the channel the cell phone is transmitting on is not known, and it is difficult in noisy conditions to determine this with enough accuracy to avoid phase wrapping.

However, the channel frequency can be removed without knowing what it is by low pass filtering the square of the correlated signal. The correlation must be squared in order to present a DC component to low pass filter. A sharp 400-order FIR low pass filter with a cutoff of half the baseband frequency (1.2288MHz) was found to be most effective in removing the channel frequency from the signal. The last step is to smooth the correlation curve using a spline function. This is required because the received data is sampled at 62.5MHz, or 16nsec between samples which does not provide enough resolution to find the time difference down to the necessary sub-nsec resolution. Finally, the peak index of each filtered and smoothly correlation is found and these indexes are converted to delays in nanoseconds using a linear function. The location of the cell phone is determined by inputting the six channel delays and the known locations of the reference antennas to Chan's algorithm, an optimal output-sensitive algorithm that computes the convex hull of a set P of n points, in two or three dimensional space.

Table 2: Analysis of received signals (same process for simulated or actual signals)

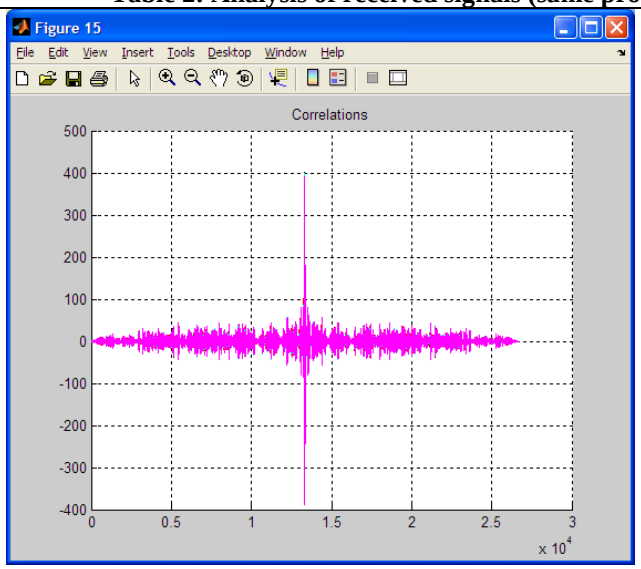


Figure 20: Correlation of signals received from two antennas.

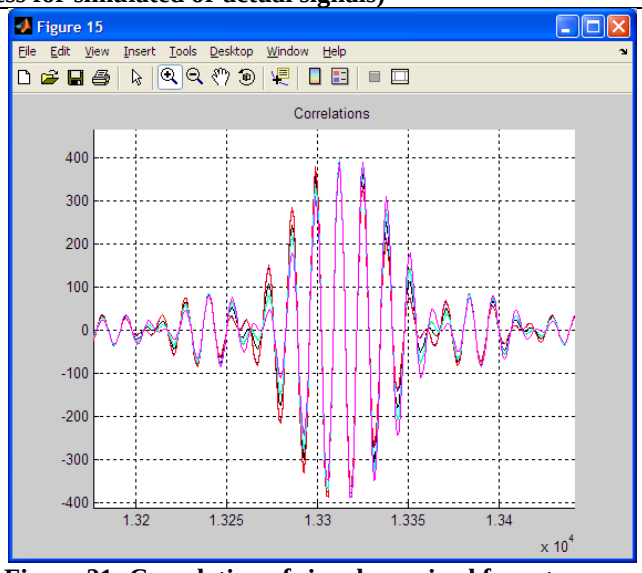


Figure 21: Correlation of signals received from two antennas, zoomed-in.

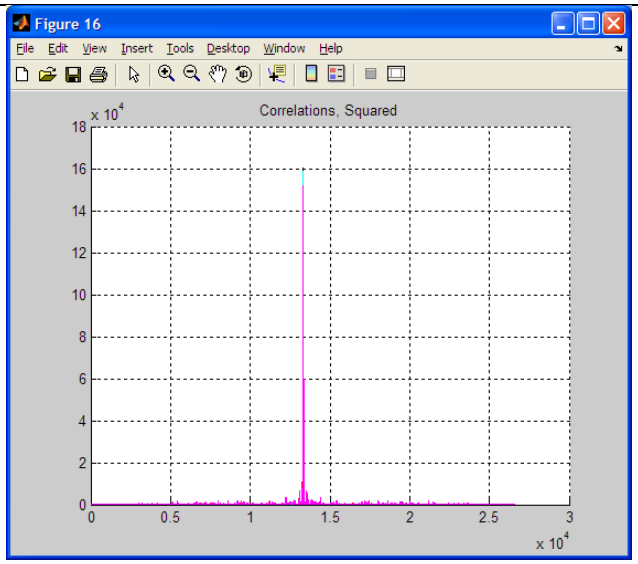


Figure 22: Correlation, squared. This is done to have a DC component to filter.

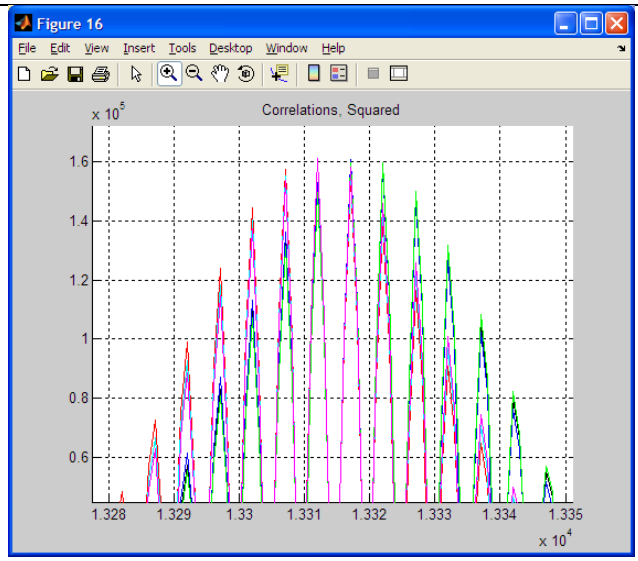


Figure 23: Correlation, squared, zoomed-in. It is clear that it would be very difficult to determine the peak index of each correlation, needed to find the time delays, without first removing the channel frequency.

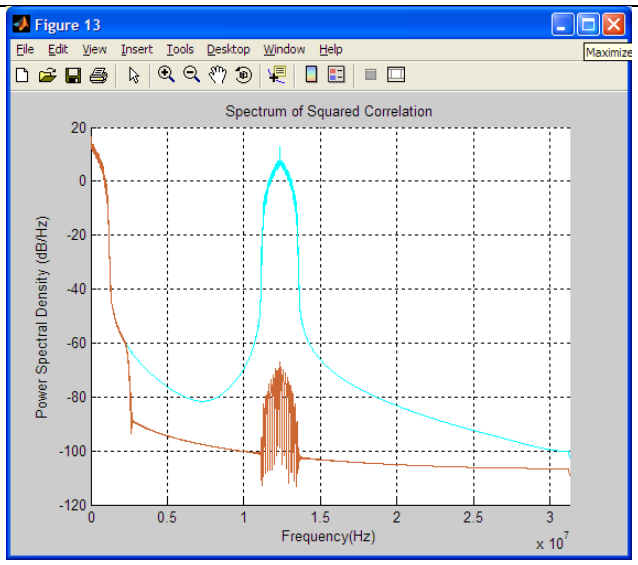


Figure 24: Spectrum of squared correlation, before and after applying 400-order FIR LPF. Note that the center blue peak – the channel frequency – has been is attenuated by about 80dB.

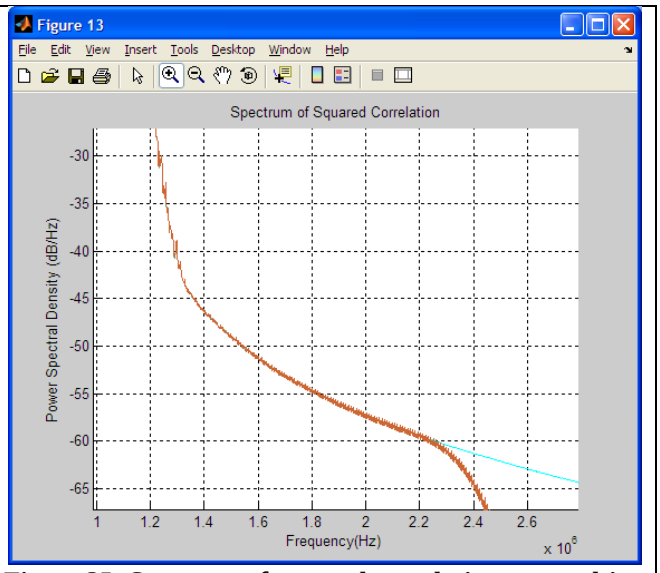


Figure 25: Spectrum of squared correlation, zoomed-in. Note that the low frequency components (the baseband signal) are well preserved.

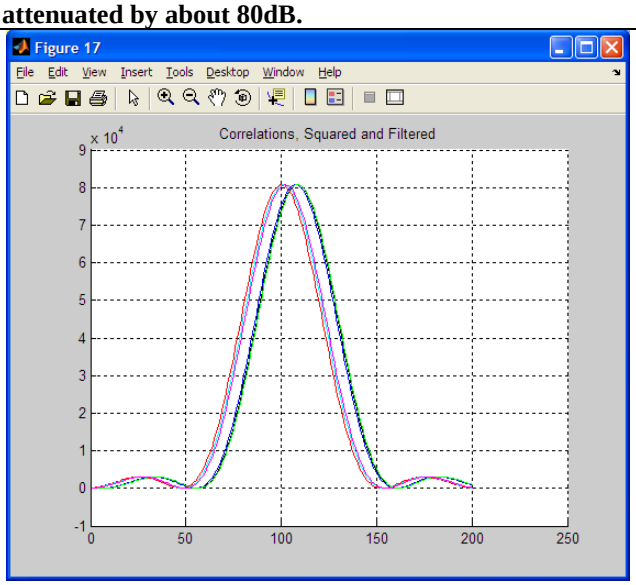


Figure 26: Correlation - squared, filtered. The channel frequency has been completely removed.

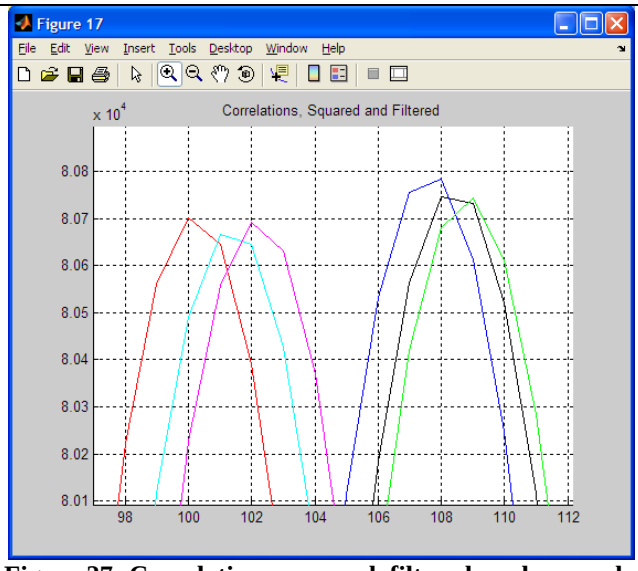


Figure 27: Correlation - squared, filtered, and zoomed-in. The time delays between the six pairs of antennas (1-2, 1-3, 1-4, 2-3, 2-4, 3-4) are now clearly visible, but the sampling is too coarse to accurately find the peaks.

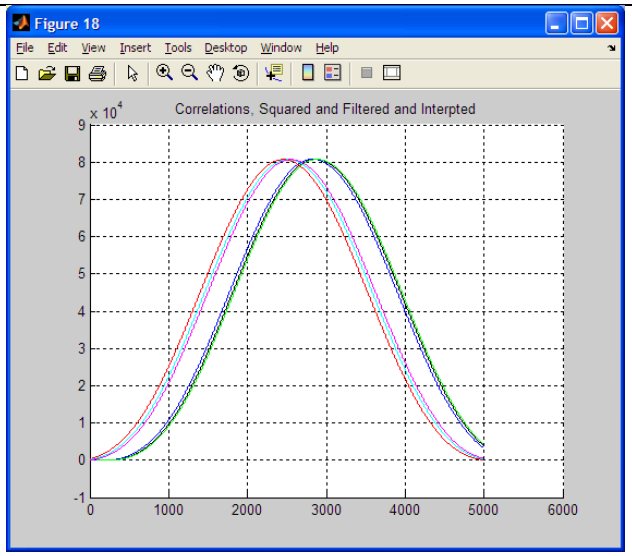


Figure 28: Correlation - squared, filtered, and after applying cubic spline interpolation.

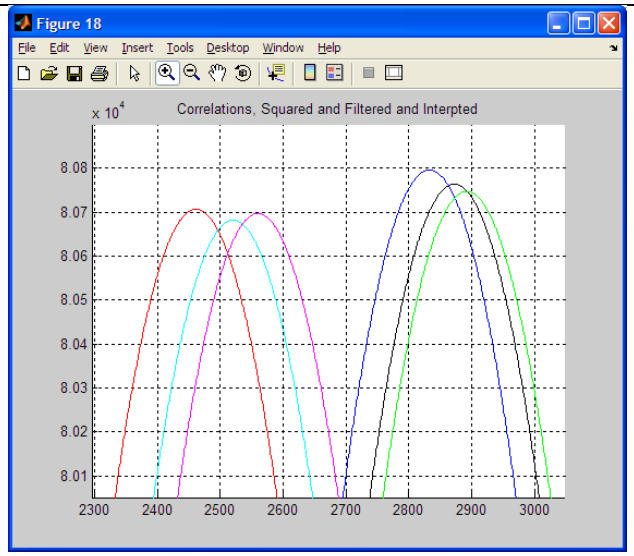


Figure 29: Same, zoomed-in. The indexes of the peaks of each correlation can now be accurately found. The differences in these indexes are converted to delays in nanoseconds using a linear function.

6. Results

6.1. Simulation Results

Cell phone location solution results using simulated CDMA2000 data have been found to be very favorable, even at low signal-to-noise ratios. A shown in Table 3, the average positioning error of the mobile is only about six feet at zero SNR, enough to locate the cell phone within one or two cells. With actual data, the SNR will be greater than 0db; however, multipath will be present which has not yet been added to the simulation.

Table 3: Performance of time different/mobile positioning algorithm with simulated data

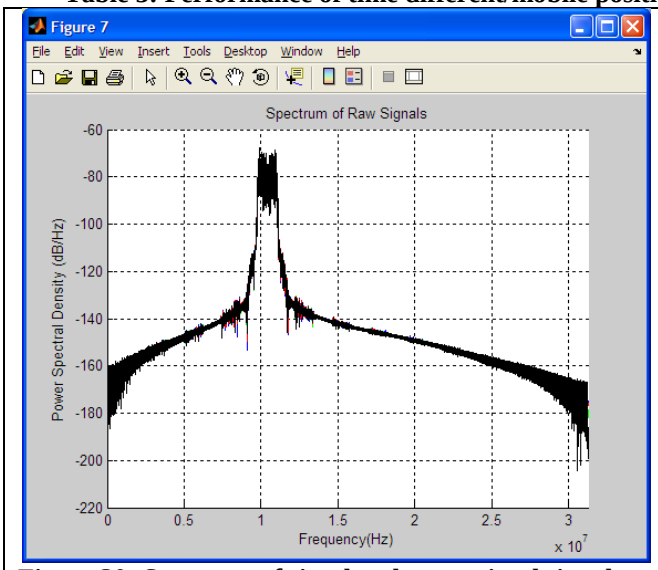


Figure 30: Spectrum of simulated transmitted signals, four antennas, with no added noise.

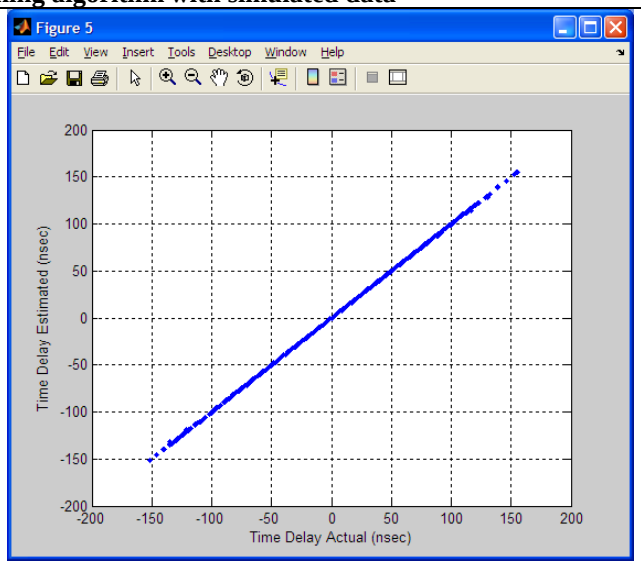


Figure 31: No added noise - relationship of time delay actual to estimated after 100 runs with channel and mobile location randomized. Time difference errors: median=0.156nsec; std=0.270nsec; worst=2.160ns. Slant position errors: median=2in; std=2in; worst= 1ft 10in.

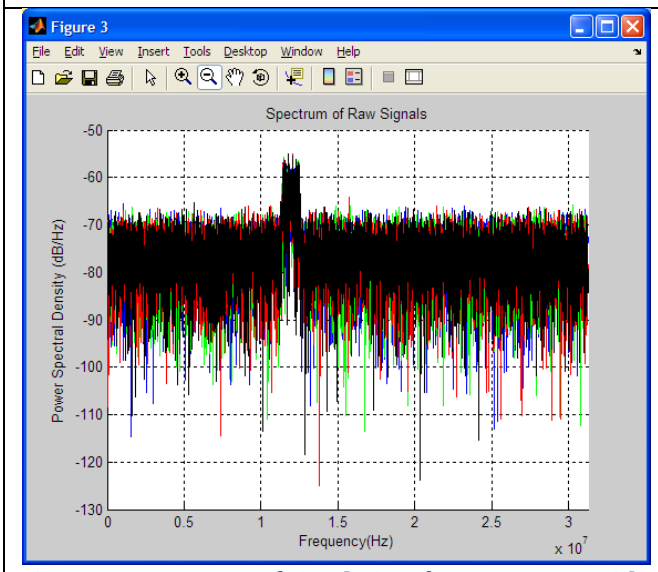


Figure 32: Spectrum of simulation, four antennas, with additive white noise added to results in SNR of 0dB.

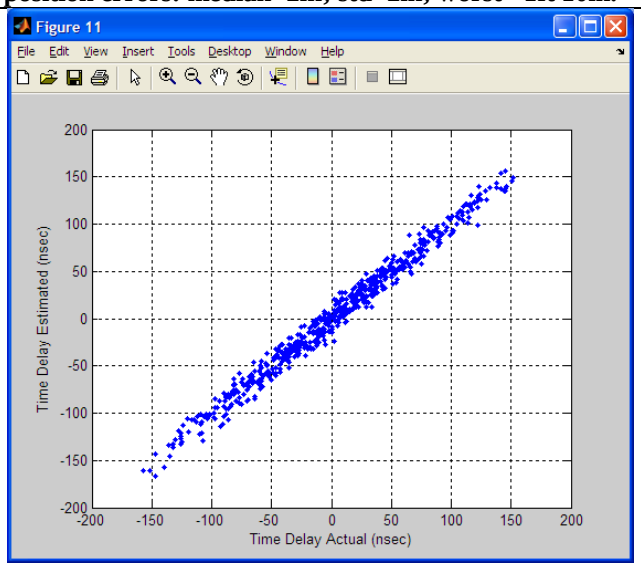


Figure 33: 0dB SNR - relationship of time delay actual to estimated after 100 runs with channel and mobile location randomized. Time difference errors: median=5.903nsec; std=4.951nsec; worst=25.614ns. Slant position errors: median=5ft 3in; std=2ft 9in; worst= 12ft 10in.

6.2. Receiving Hardware Results

Preliminary tests have been done with the receiving hardware built during this performance period. Tests have been performed both with a flip phone (LG VX5500) and with a cellular modem (MultiTech MTCBA-C1) both which used the CDMA2000 cellular protocol over the Verizon network. The advantages of the cellular modem are it

has a SMA connector to allow for direct wired hook-up to the hardware. This is very useful to controlled testing and to calibration out differences in cable length.

Figure 34: CDMA2000 flip phone, Model LG VX8600

Figure 35: CDMA2000 modem

Preliminary tests performed to data are as follows. First, all inputs were terminated and data collected to measure the noise floor. Then, four 164ft RG-400 cables were attached to the modem via a 4-way splitter and 60dB attenuator to verify that the signals were being received correctly and to calibrate out small differences in cable length. Next, the modem was replaced with one antenna to test the reception of signals through-air. Finally, antennas were connected to the ends of each of the four cables and extended 30-60 feet away and data was collected to determine the sensitivity of the energy detection algorithm. The above is illustrated in the below photos and in Table 4.

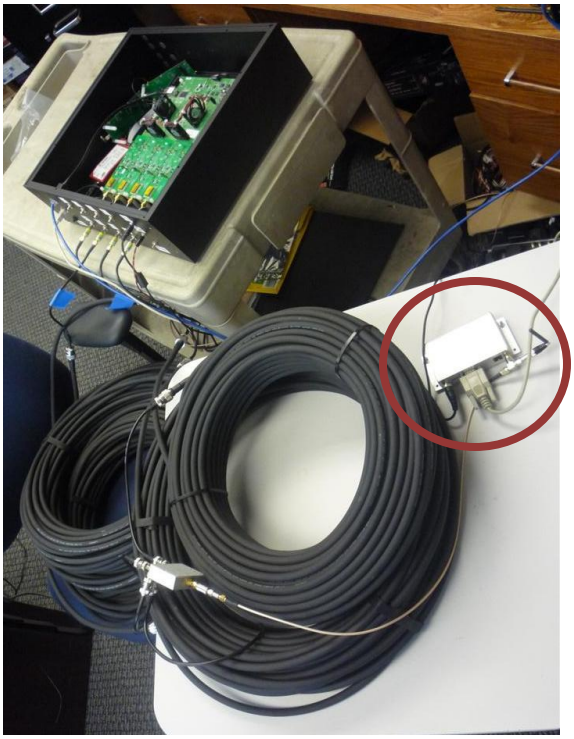


Figure 36: Connected to modem

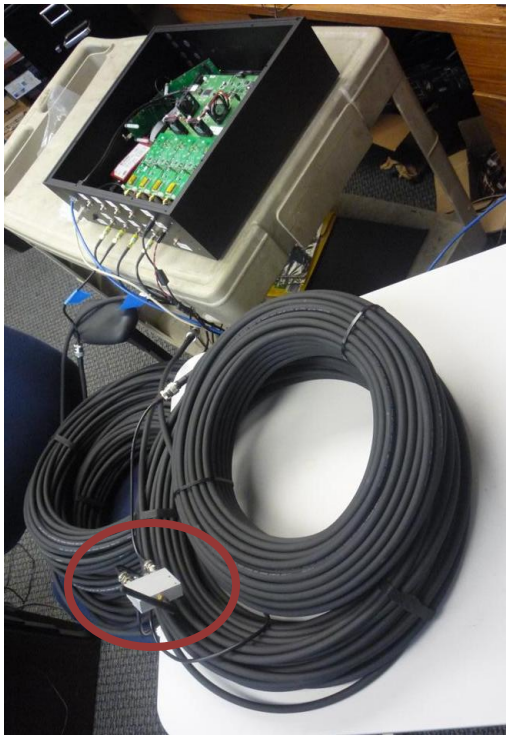


Figure 37: Connected to single antenna

Table 4: Results of preliminary data collection from receiver hardware.

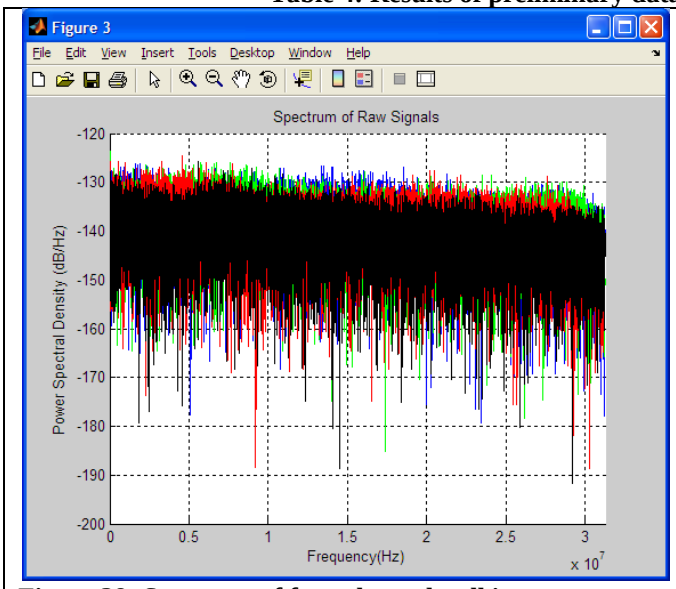


Figure 38: Spectrum of four channels, all inputs terminated.

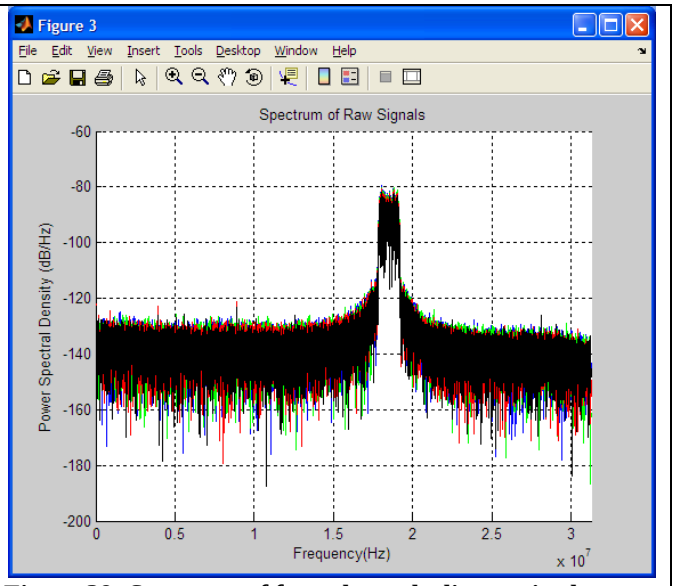


Figure 39: Spectrum of four channels direct-wired to output of modem via a four way splitter (60dB attenuation added).

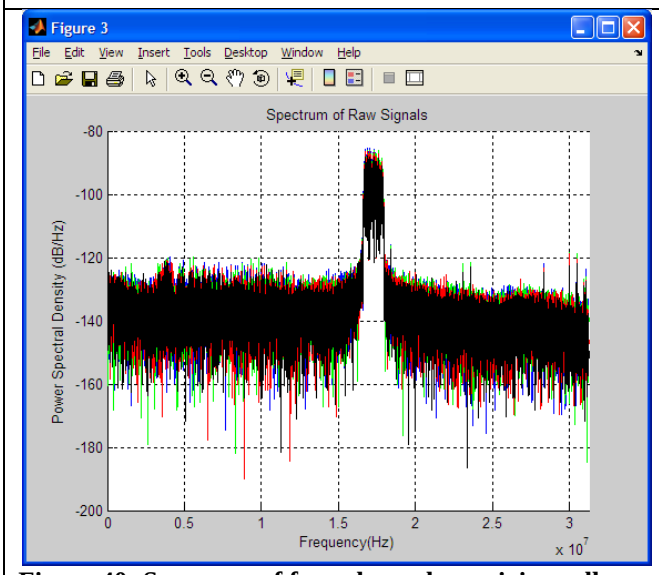


Figure 40: Spectrum of four channels receiving cell phone signals through air in same room, received by single antenna connected to 4-way splitter.

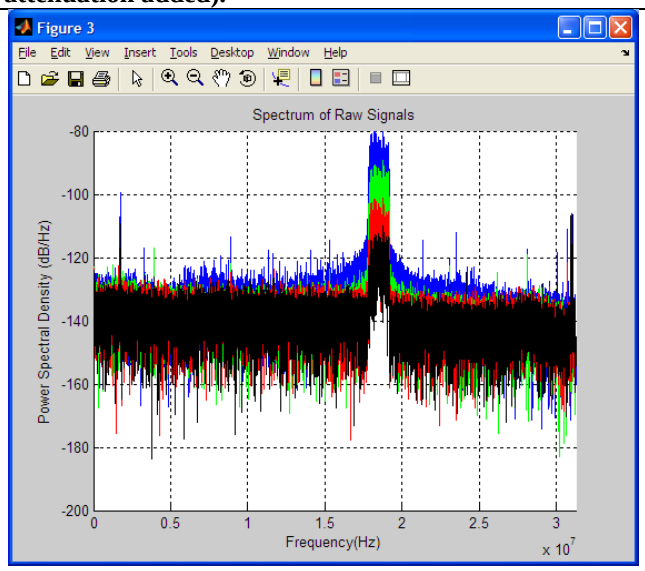


Figure 41: Spectrum of four channels, received by antennas 30-60ft from modem, indoors, non LOS

7. Improvements to System

Based on the above results collected during the third performance period, improvements were identified and implemented in the FPGA code during the fourth performance period, which has significantly improved system performance.

The following issues were noticed while performing data collection with the CDMA2000 cell phone and modem:

1) The threshold at which the system reliably triggered was at SNR of 20dB SNR below that there would be either false positives or false negatives,

2) The fact that the system would trigger on any signal in the 824-849MHz channel – a desirable feature for the final system - made testing difficult due to signals from other cell phones,
3) There was crosstalk between the four channels, particularly between adjacent receiver boards (1&2, 2&3, and 3&4). Changes to remedy each of these issues have been made, and preliminary tests have shown marked improvement in each area.

The first issue of the trigger not working well below 20dB was solved by using a frequency domain method of triggering instead of a time domain one. Since we know the exact bandwidth of the CDMA signal (1.2288MHz), this improves sensitivity significantly. We can now detect cell phone signals near 0dB SNR and false triggers are very rare. Detection of a weak signal can be seen in Figure 42.

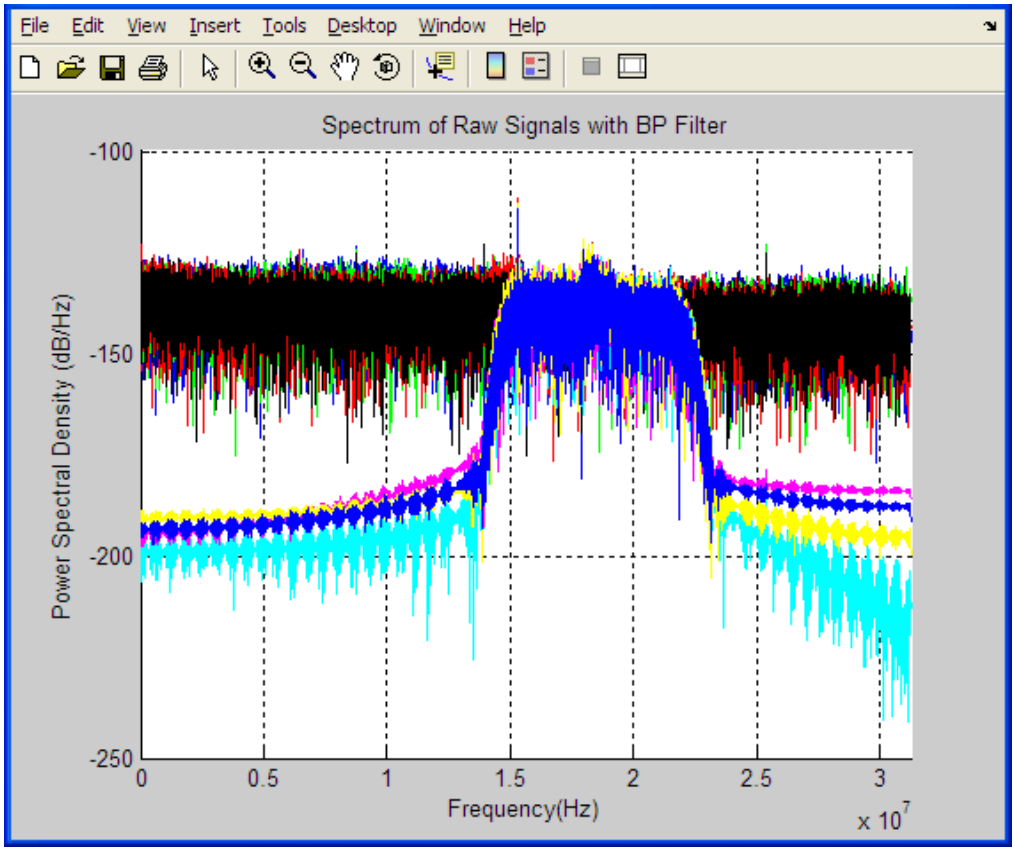


Figure 42: Detection of very weak cell phone signal

The second issue of selective triggering was solved by providing the option of only trigging in a particular band. For example, a command can be sent down to the FPGA to trigger anywhere from 838MHz to 841MHz. In our typical test scenario, this covers the three bands our flip phone and modem use, while blocking out other bands, thus allowing us to ensure that transmissions are coming from the cooperative transmitter. A related option is to restrict triggering to signals with a greater than a particular bandwidth, thus allowing us to only trigger on CDMA2000, and not GSM. We found this option works well; however, a very strong GSM signal can still trigger the system.

The third issue of the crosstalk between channels was improved by moving the receiver board to different slots on the ADP-1000 processor board to maximum the distance between them (Figure 43). This eliminates the crosstalk problem except in case where transmitter less than ~1ft from the receiver, which could not happen in practice. This is shown in Figure 44 and Figure 45.

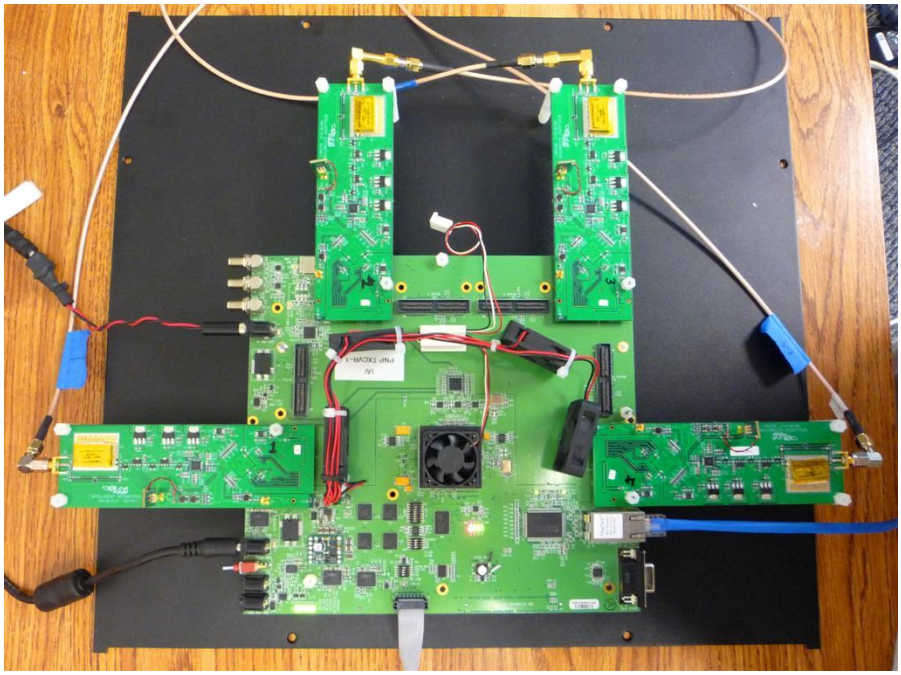
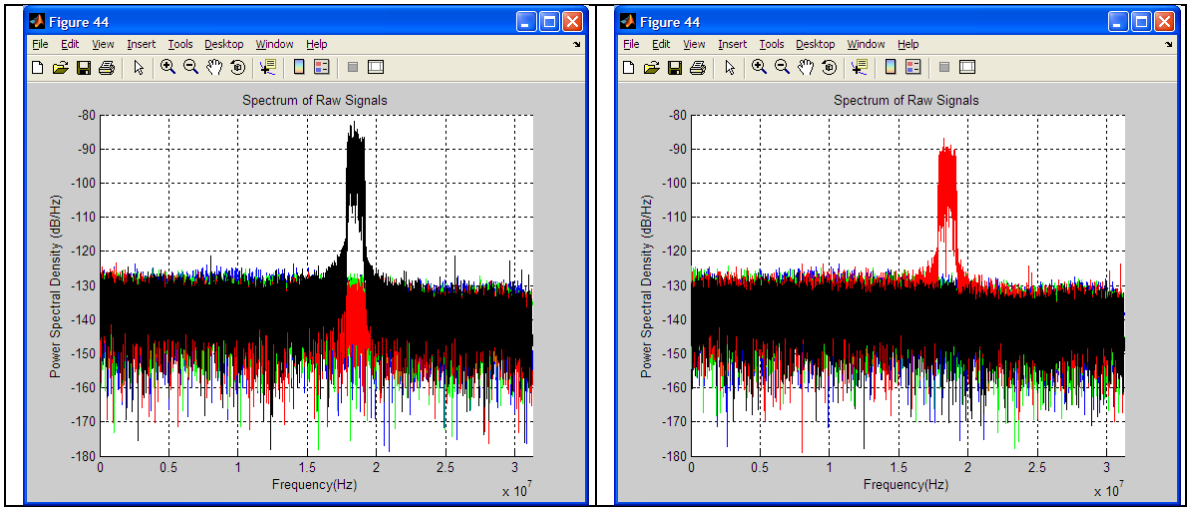


Figure 43: Cell phone receiver board, with front end receiver modules placed to minimize crosstalk



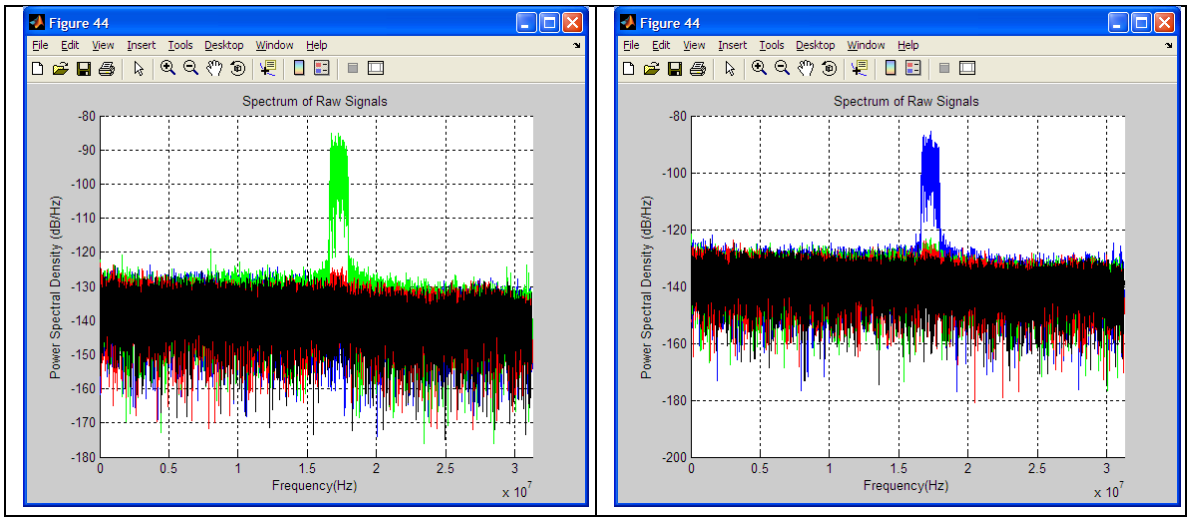


Figure 44: Test of crosstalk between channels. Cell phone text message placed with phone about 2ft from antenna placed in another room while the other three channels are terminated. There is no evidence of crosstalk on the other three channels even with an SNR of 35dB.

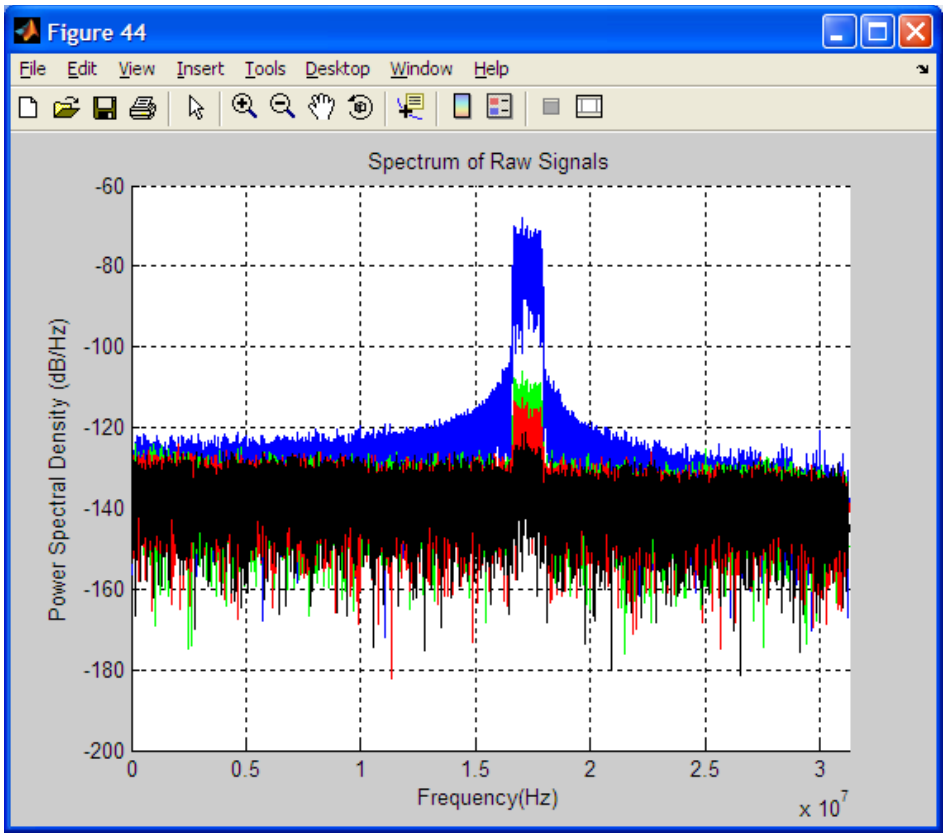


Figure 45: Identical setup as above, but this time with cell phone placed six inches from the receiving antenna. At this SNR of 55dB (which is 7dB below the received saturation limit) crosstalk is evident.

8. Products

Under this project, we have developed a novel technique for locating cellphone use in an indoor environment. A hardware instrument and software package that implements the

technique has been developed. A data base containing representative cell phone signals for indoor environments has been established.

9. Participants & other Collaborating Organizations

We provide a overview of IAI staff that contributed to the project in Table 5 below.

Table 5. IAI project staff.

Name	Project Role	Contribution to project	Funding Support	Collaborated with individual in foreign country
Eric van Doorn	PI	Program lead	DARPA, ONR	No
Biswadip Dey	Summer intern	Algorithm Development, Data Collection	DOT	No
Zhitong Guo	Engineer	Data collection and analysis	DOT	No

Results of the project have been briefed to potential end users and Department of Defense prime contractors to facilitate transition to the end user.

10. Impact

Impact on the development of the principal discipline(s) of the project

The impact of the project on the criminal justice system will be to offer a technology solution that can (partially) address the issue of cell phone use in correctional institutions.

What is the impact on other disciplines

"Nothing to Report."

Impact on the development of human resources

"Nothing to Report."

Impact on physical, institutional, and information resources that form infrastructure

Using the instrumentation developed under this project, we are able to study cell phone use in other settings, such as texting in motor vehicles.

Impact on technology transfer

To date the technology has not been transitioned.

Impact on society beyond science and technology

"Nothing to Report."

Dollar amount of the award's budget is being spent in foreign country(ies)

$0.

11. Changes/Problems

"Nothing to Report."

12. Budgetary Information

"Nothing to Report."

13. Conclusions

We believe we now have a high performing system for capable of locating CDMA2000 cell phones using time different of arrival techniques. We will first test using TDOA indoor, if this does not work sufficiently due to multipath, the Matlab code will be modified to use fingerprinted calibration instead. This change will require no changes to the hardware or FPGA code.