UWB Enhanced Time Difference of Arrival System

Summary

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.

Contents

Research Objectives

The purpose of the proposed technology development and evaluation effort is to design, implement and test an effective system for the detection and localization of cellular phones in correctional facilities. Correction officials have identified the problem of cell phones in prisons as one of the toughest issues they face. The phones, smuggled in by guards or family members and activated with hard-to-trace prepaid calling plans, are a lifeline for criminals and gang members to order hits, buy drugs and plan escape attempts from behind bars. We are developing a prototype Time Difference Of Arrival (TDOA) emitter detection and location system, and ultimately will demonstrate the system at Lawrenceville Correctional Center. The demonstrated system will be capable of detecting and locating cell phones in real time.

Correctional facilities differ in size and layout, and specific layouts such as the 1950 telephone pole design, the 1980 skyscraper design, or the 1990 modular design may require different number and different placement of TDOA nodes. Our first objective in this study was to identify in close collaboration with NIJ staff, an appropriate site for system evaluation. A site within driving distance, of limited scale, with staff motivated to participate in system evaluation would be most desirable. As part of this objective we intended to learn from the facilities staff how the cell phone problem is manifesting itself in their facility. For instance, are particular cell phone

types (such as very small phones with prepaid plans, particular carriers) more prevalent? Are there specific locations that have been identified or suspected of being used for cell phone conversations? How many cell phones might be operated at any given time? How long might each be operated? What other emitters, such as guard radios, may be active at the facility? How should the human interface to the cell phone detection and location system be designed? How could an instrumentation, test, and evaluation effort be conducted with the least interference to normal facility operations?

The next objective was to survey the site to determine its RF propagation characteristics, both for cell phone signals, and the signals our system uses for synchronization and data transfer. From a technical point of view, this would be best accomplished by operating cell phones inside the facility, and measuring the received signals at various locations outside the building. The purpose of these measurements is to understand the requirements for receiver sensitivity, transmit power/frequency, and other system characteristics, as well as desired locations for TDOA node placement. If a three dimensional floor plan is available, these measurements can be used with mature simulation tools [Biaz2005, WinProp] to provide very accurate predictions of received signals at locations in and around the building that were not surveyed, helping to minimize need to disrupt day to day operations at the facility. The results of these studies, when published, can inform any method that seeks to detect, locate or jam cell phones in penitentiaries.

The third objective is to develop instrumentation that can detect and acquire cell phone signals with nanosecond resolution at multiple points on a floor or throughout a building, and use this system in our own facility to acquire test data, calibrate the systems, and develop algorithms.

The final objective to present our results in professional conferences and/or suitable peer reviewed journals.

Results, findings and conclusions

RF propagation and characteristics

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. 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.

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.

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.

Hardware Design

The initial system design 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.

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.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.

Simulation of CDMA2000 transmission

The method used to generate signals similar to those received from the receiving hardware is as follows: 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.

Determining time difference and cell phone location

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 b 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.

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 that 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

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 threshold at which the system reliably triggered was at SNR of 20dB SNR below that there would be either false positives or false negatives,
3) 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,
4) 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.

Data collection

Data collection has started at IAI's facility. Data will be collected for approximately 20 offices on a single floor. Multiple measurements per office will be collected. RF finger printing algorithms will be developed, specifically:

Comparison between Auto- and Cross-correlation of calibration measurements with those collected with phone at unknown location. We will use data reduction methods, such as Support Vector machine, and Principal Component Analysis to reduce the dimensionality of the look up table.

In this study we will:

-quantify the need for calibration data vs. the achievable accuracy

-determine how often calibrations have to be repeated

-determine how many receiver channels are needed per unit area of floor plan to be monitored.

-determine guidelines for optimal placement of receiver antennas.

Implications for criminal justice operations

In this section we will describe how the results obtained in this study determine the feasibility and practicality of the proposed solution. Specifically, we will answer the following questions:

-What is the achievable detection rates and location accuracy of the proposed system?

-What is an achievable system hardware cost, and expected cost of ownership over the lifetime of the system?

-How much calibration effort is needed at installation, and how much re-calibration effort is needed to maintain the system performance?