The author(s) shown below used Federal funds provided by the U.S. Department of Justice and prepared the following final report:

Document Title:	**Time Difference of Arrival System for Cell Phone Localization in Correctional Facilities**
Author(s):	**Eric van Doorn, Ph.D., Arvind Bhat, Benjamin Lonske, Zhitong Guo, Pedram Hovareshti, Ph. D., Siddarth Gaddam**
Document No.:	**248828**
Date Received:	**May 2015**
Award Number:	**2011-IJ-CX-K002**

This report has not been published by the U.S. Department of Justice. To provide better customer service, NCJRS has made this federally funded grant report available electronically.

Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

Intelligent Automation Incorporated

Time Difference of Arrival System for Cell Phone Localization in Correctional Facilities

Final Report

Contract No. # 2011-IJ-CX-K002
Sponsored by: National Institute of Justice
COTR/TPOC: Dr. Frances Scott, Frances.Scott@usdoj.gov, (202) 305-9950

Prepared by

Eric van Doorn, Ph.D. – PI

Arvind Bhat,

Benjamin Lonske,

Zhitong Guo,

Pedram Hovareshti, Ph. D.

Siddarth Gaddam

This project was supported by Award No. 2011-IJ-CX-K002 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.

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

PROJECT SUMMARY

In this cell phone tracking project, both hardware and software were developed. We completed the design of portable hardware, and made progress towards integration of the hardware components. Finally, we filed a patent in order to protect the intellectual property developed under this project. From the software side, we finished the development of a RF-fingerprinting approach to locating cell phones in prison. We also developed a GUI for the final demo, and performed extensive experiment testing.

The hardware is using a single data collection unit and multiple cabled antennas that extend from the receive ports to antennas located at the corners of a prison facility building. We redesigned the hardware to make it compatible with sensing phones in all three cell phone bands used in the US. This was performed using the four channel FPGA-based hardware designed for the multiple bands (CDMA2000, WCDMA and GSM). During the subject period of performance, we performed extensive testing of the developed system at the IAI office site for the 850MHz, 1700MHz and 1900MHz bands.

From the software side, we examined the use of a classification-type approach to locating cell phones in prison. Extensive data was collected in IAI’s facilities and analyzed in an office environment and the testing results are very encouraging. These data were collected to train and optimize the detection and localization algorithms. The date was also used in an analysis to estimate the maximum coverage area that could be achieved with the current hardware.

The redesigned hardware receiver box and its GUI were demonstrated to Dr. Francis Scot from NIJ, and several staff from the Harris Corporation.

ACKNOWLEDGEMENTS

We thank Frances Scott for her encouragement and support.

LIST OF CONTENTS

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

LIST OF FIGURES

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

LIST OF TABLES

1. Introduction and Background

Cell 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. Correction officials have identified the problem of cell phones in prisons as one of the toughest issues they face. The purpose of this project is to design, implement and test an effective system for the detection and localization of cellular phones in correctional facilities. The key purpose of the proposed effort is to mature the prototype Time Difference Of Arrival (TDOA) and signal strength detection for location system from laboratory to deployment in a correctional facility, and capable of detecting and locating cell phones in real time. Another key purpose is to explicitly use the known building floor plan in the algorithm that processes the received cell phone signals in to the likely location.

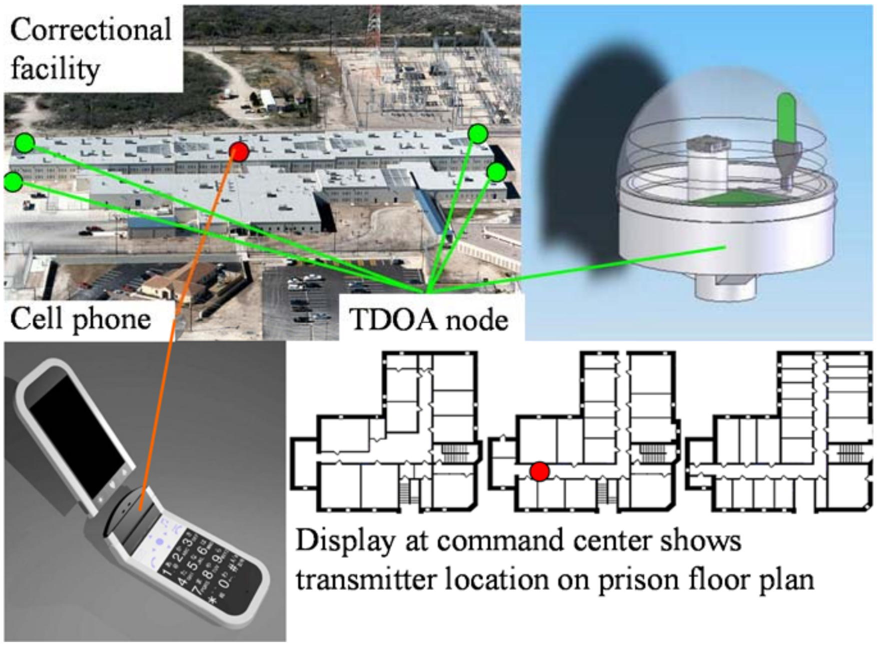

Correctional facility
Cell phone
TDOA node
Display at command center shows transmitter location on prison floor plan

Figure 1. TDOA system for real-time cell phone detection and localization in correctional institutions.

The high level diagram of the detection system is shown in Figure 1. The system consists of four antennas located on the building outside or inside walls, which generate three TDOA signals and four signal strength signals. Based on such information, the estimated cell phone location is reported to a laptop computer or a handhold device where they are displayed super imposed on a prison floor plan.

1.1 Review of Relevant Literature

Previously, in the application for the ongoing work, we motivated the our choice of using the Time Difference Of Arrival (TDOA) method for localizing cell phones in buildings, over other methods such as RF sniffing, and Direction Of Arrival. Here we will focus on how the TDOA algorithm that processes the received cell phone signals can be improved by using the building floor map explicitly.

We show a schematic of a TDOA setup in Figure 2. In essence, several RF receivers (with known locations) are tightly synchronized, and used to detect the RF emission of the source to be tracked at several locations. In an environment without strong reflectors, the receiver locations, the time differences of the signal's arrival and the known speed of propagation (1ft/ns), can readily be used to determine the location of the RF source (cell phone etc.). However, any building, and especially correctional facilities incorporating concrete and metal, the cell phone signal will get reflected very strongly, and the relationship between the received signals and the location of the cell phone is complex. There has been extensive analysis of the effect of multipath on TDOA performance [Yuan1995, Qi2006]. Thus, multipath can cause 1) weak signal in the receiver due to Line Of Sight (LOS) and or reflections to cancel each other, 2) wrong (too long) estimate of TDOA because only multipath reaches the receiver (LOS is blocked completely), and 3) distortion of the waveform if LOS and first multipath arrive within the rise time of the signal of each other (as little as 20 nanoseconds for cell phones). Channel multipath can be measured using sliding vector correlation techniques [Anderson2002], and we have designed similar techniques to measure channel characteristics in the selected site to determine how strong the impact of multipath might be. However, channel characteristics could vary rapidly for different locations of both the emitter and the receiver. It is prohibitively labor-intensive to measure the channel multipath for all possible configurations of TDOA and cell phone locations.

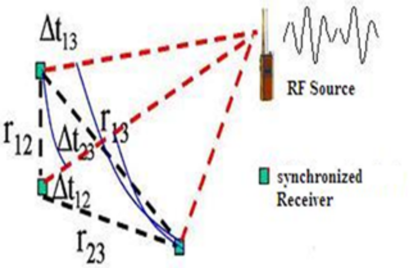


Figure 2: TDOA for tracking RF emission

1.2 FCC Compliance.

Keeping compliance with the Federal Communication Commission (FCC) regulations in mind is of key importance to avoid showstoppers later. We are fully cognizant of Title 47 and its implications and our development path is aimed straight at a fully FCC compliant, scalable solution. Importantly, we do NOT interfere with cell phone signals. Since our antennas only receive cell phone signals, eliminating the last remaining issue with FCC compliance.

1.3 Implications for Policy and Practice

While the Phase II effort focuses on the localization of cell phones, in practice the current IAI effort funded by NIJ is also being developing while keeping in mind other applications of portable ad-hoc deployable systems for outdoor emitter location. As such, the system we are developing has law enforcement applications well beyond the prison-cell phone issue. The system design we are proposing is innovative, portable, deployable standalone or suitable for integration with any commercial radio sub-systems. The key law enforcement areas and homeland security areas where the technology can be leveraged are:

- Tracking suspects using cell/cordless phones inside buildings, monitoring of building facilities or suspect areas for cordless/cell phone users

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

- Tracking EMS personnel (firefighters, police, medical), SWAT/ATF/FBI/undercover agents, as well as staff inside correctional facilities and security guards inside structures by means of the communications equipment they are already using (no added burden).
- Tracking assets such as (unmanned) vehicles
- Law enforcement may also be involved in search and rescue operations (recent operations on Mt. Hood to locate stranded climbers would have benefited greatly from the technology proposed here).

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

2. Hardware Receiver System Development

The RF receiver box is designed as a four-channel single-stage heterodyne receiver, which detailed block diagram is shown in Figure 3; while Figure 4shows prototype hardware box. The receiver design for all four channels is identical. This hardware down-converts the received RF signals to an IF frequency and it is capable of being configured to any of the 3 cell phone bands (850MHz, 1700MHZ and 1900MHz) in the US by replacing the front end RF filters (which are located in-line with the receive antennas), and by providing a suitable Local Oscillator frequency (provided by a flexible signal generator and later replaced by a compact size signal generator board).

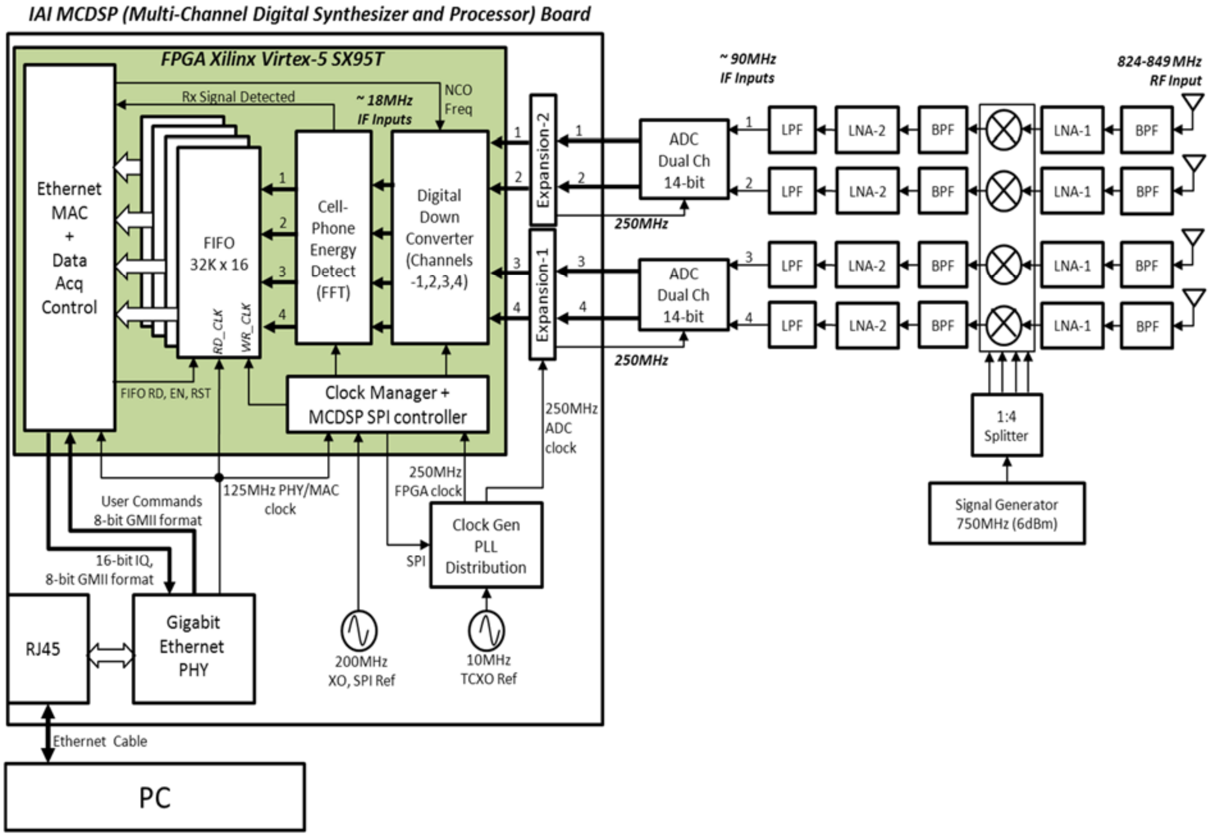

IAI MCDSP (Multi-Channel Digital Synthesizer and Processor) Board
FPGA Xilinx Virtex-5 SX95T
Rx Signal Detected
~ 18MHz IF Inputs
NCO Freq
Ethernet MAC + Data Acq Control
FIFO 32K x 16
RD_CLK
WR_CLK
Cell-Phone Energy Detect (FFT)
Digital Down Converter (Channels -1,2,3,4)
Expansion-2
Expansion-1
1
2
3
4
ADC Dual Ch 14-bit
250MHz
~ 90MHz IF Inputs
LPF
LNA-2
BPF
LNA-1
BPF
824-849 MHz RF Input
1:4 Splitter
Signal Generator 750MHz (6dBm)
FIFO RD, EN, RST
Clock Manager + MCDSP SPI controller
250MHz ADC clock
250MHz FPGA clock
125MHz PHY/MAC clock
User Commands 8-bit GMII format
16-bit IQ, 8-bit GMII format
SPI
Clock Gen PLL Distribution
RJ45
Gigabit Ethernet PHY
200MHz XO, SPI Ref
10MHz TCXO Ref
Ethernet Cable
PC

Figure 3: Detailed hardware design

The receiving system consists of one receiver/processor along with four antenna ports and four channels. The receiver board contains the following major components:

- A front-end direct conversion component for sampling signals in the RF band, low noise amplification, and band pass filtering to ~ *90MHz*
- IAI Multi-Channel Digital Synthesizer and Processor (MCDSP) Board to further down-convert the RF signal to ~ *18MHz*, perform cell-phone energy based detection algorithm, and send the information to PC via Ethernet MAC.

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

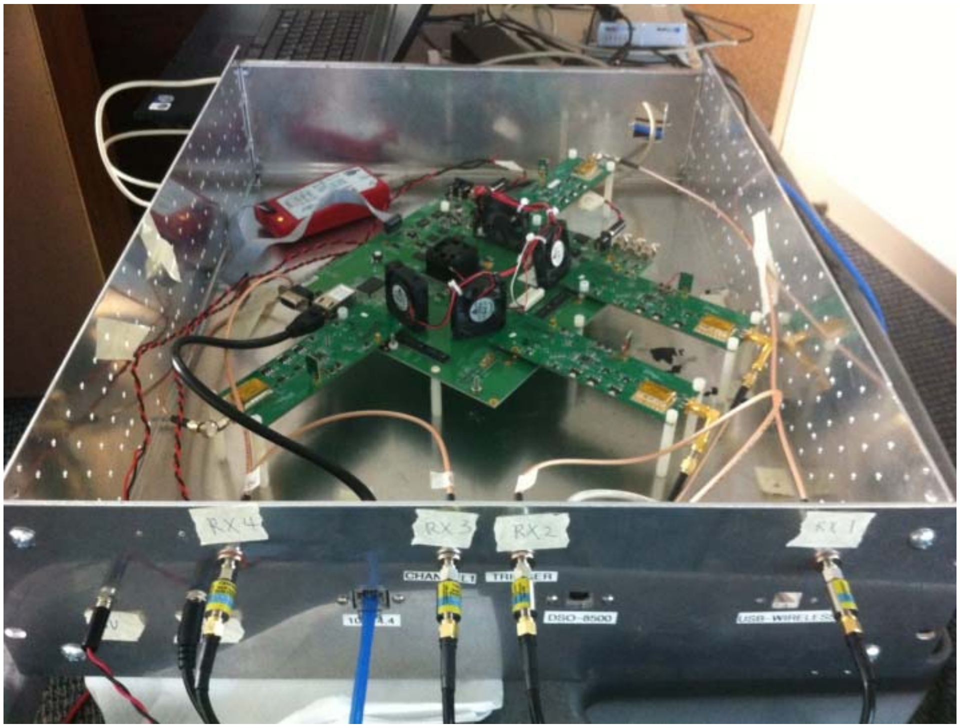


Figure 4: The 4-channel receiver/processor developed by IAI, prototype and product.

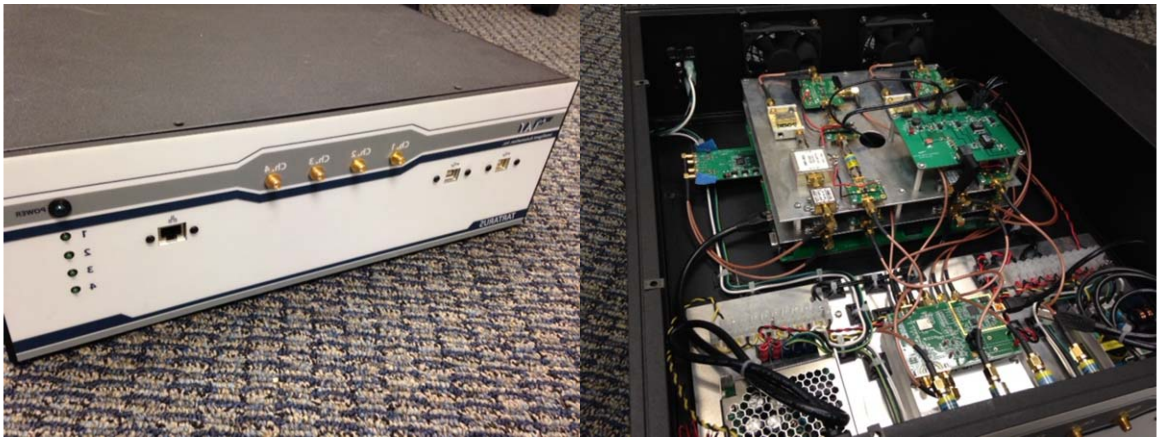


Figure 5: Final developed product with enclosure

For 850MHz band receiver shown in Figure 5, the cellular band of interest occupies approximately 25 MHz of spectrum from 824-849 MHz. A single cell phone channel occupies roughly 1.25MHz bandwidth around the carrier frequency. At each channel an RF Band-pass filter (BPF) is used to reject out-of-band noise. The RF Front-end down-converts the 824-849 MHz spectrum to intermediate frequency ranges of 74-99 MHz by mixing with a 750MHz Local Oscillator (LO). This 25 MHz IF bandwidth (from 74-99 MHz) is filtered using an IF BPF. Additional gain is provided at the IF stage and filtered again using an IF Low-pass filter (LPF). The analog IF is then sampled at 250MHz clocking speed using high-speed ADC. The processor used is Virtex-5 FPGA. It accepts sampled IF data from four independent channels at 250MHz clocking speed and 14-bit resolution each. Data is sent up to a PC running MATLAB via Gigabit Ethernet.

2.1 Multi-Channel Digital Synthesizer and Processor

The Multi-channel Digital Synthesizer and Processor (MCDSP) module was developed under an AFRL Phase-II program (#FA8650-10-C-1737). The MCDSP hardware is shown in Figure 6below.

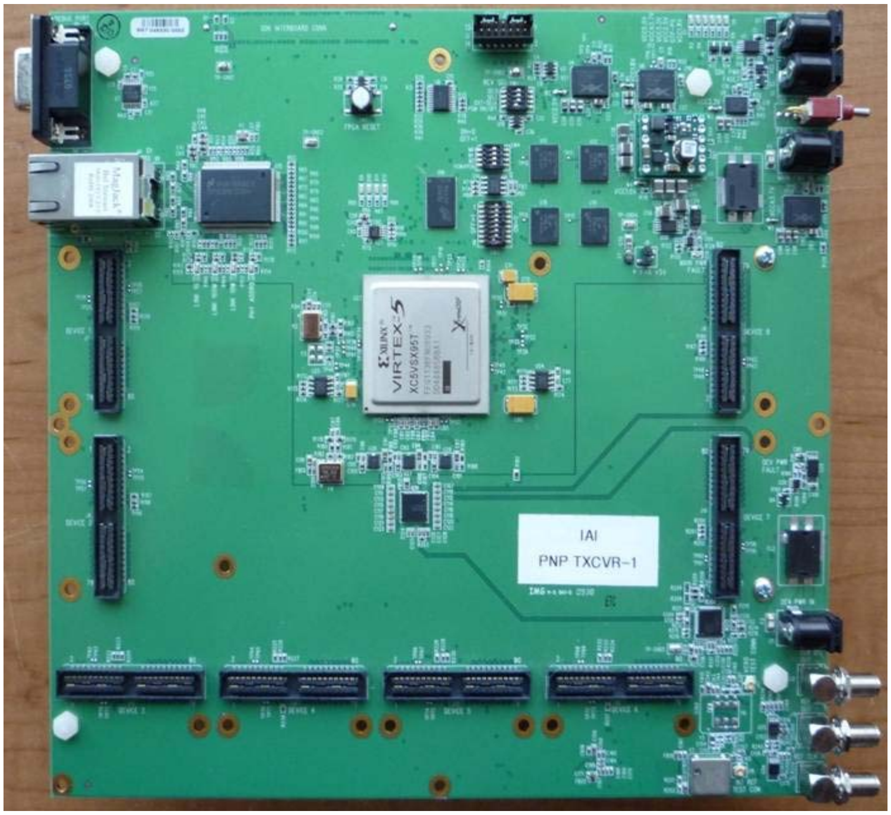


Figure 6: The MCDSP FPGA module

The key features of the MCDSP are as follows:

- Xilinx Virtex-5 FPGA for digital transceiver design.
  - Xilinx Virtex-5 LX110T, LX155T, SX95T (currently on-board), FX70T, FX100T in FFG1136 package.
- On-board Clock/RF synthesizer covers 137.5 MHz to 4GHz frequency band.
- Dimensions: 8.75” x 8”.
- Eight high-density Samtec-QSH 80 pin expansion slots, with 16 bit differential data bus, 2 differential clock pairs and GPIO for control.
- Up to 1.2 GHz LVPCEL Clock distributions on board to each expansion slot.
- Two RocketIO GTP transceivers for multi-gigabit serial data transfer between MCDSP modules.
- RS232 and 10/100/1000 Ethernet PHY as open interfaces.
- On-board 64MB DDR2 SDRAM for burst-mode radar processing.

- Standard EMIF (Extended Memory Interface) interface connector to interface external DSP processors or General Purpose Processors.
- On-board high stability 10 MHz TCXO reference (can be phase-locked to an optional external 10 MHz reference). Thus multiple modules can be phase synchronized.
- JTAG interface and Four-XCF32P Platform Flash PROM for FPGA configuration. At least 3 (for XC5VSX95T) configurations can be stored, which can be selected on-board for multi-mode operations.

2.1.1 MCDSP Block Diagram

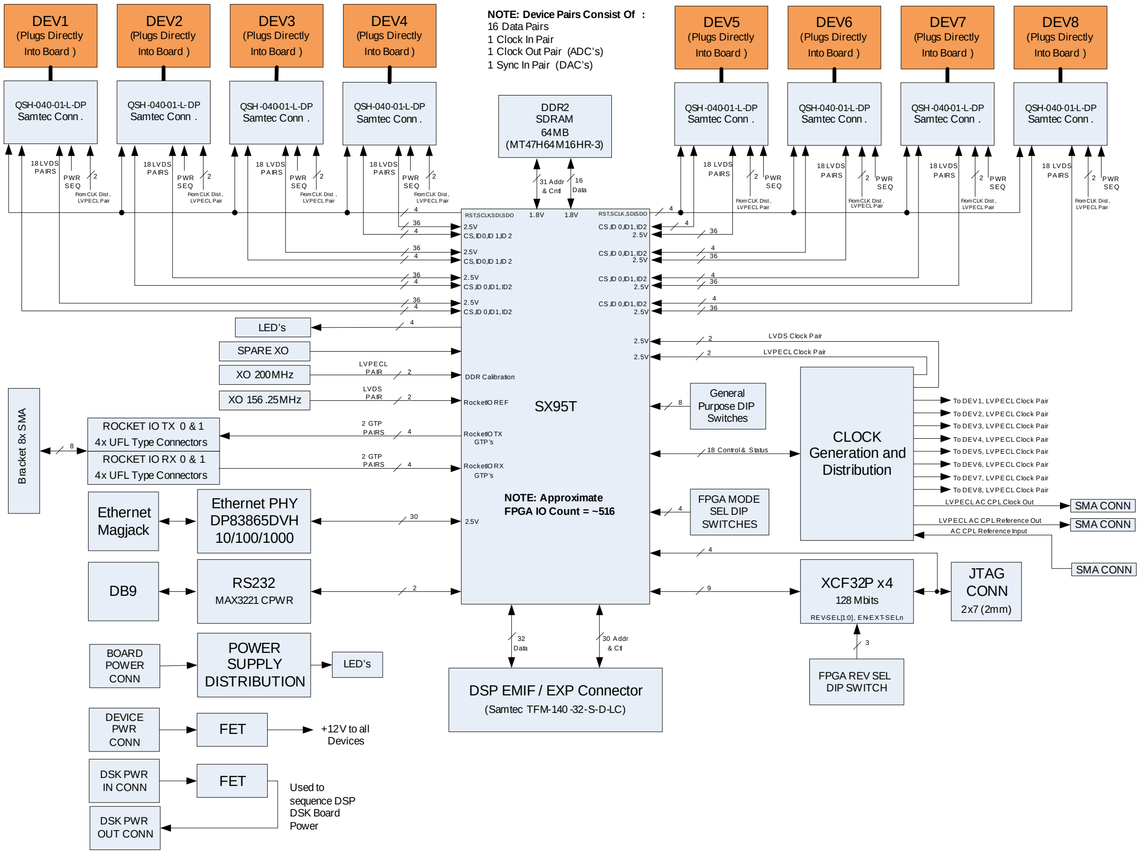

DEV1 (Plugs Directly Into Board)
DEV2 (Plugs Directly Into Board)
DEV3 (Plugs Directly Into Board)
DEV4 (Plugs Directly Into Board)
DEV5 (Plugs Directly Into Board)
DEV6 (Plugs Directly Into Board)
DEV7 (Plugs Directly Into Board)
DEV8 (Plugs Directly Into Board)
NOTE: Device Pairs Consist Of :
16 Data Pairs
1 Clock In Pair
1 Clock Out Pair (ADC's)
1 Sync In Pair (DAC's)
QSH-040-01-L-DP Samtec Conn .
18 LVDS PAIRS
PWR SEQ
2
From CLK Dist , LVPECL Pair
DDR2 SDRAM 64MB (MT47H64M16HR-3)
31 Addr & Cntl
16 Data
1.8V
1.8V
RST,SCLK,SDI,SDO
4
36
2.5V
CS,ID0,ID 1,ID 2
CS,ID 0,ID1,ID2
LED's
SPARE XO
XO 200MHz
LVPECL PAIR
XO 156 .25MHz
LVDS PAIR
DDR Calibration
RocketIO REF
SX95T
Bracket 8x SMA
8
ROCKET IO TX 0 & 1 4x UFL Type Connectors
ROCKET IO RX 0 & 1 4x UFL Type Connectors
2 GTP PAIRS
RocketIO TX GTP's
RocketIO RX GTP's
NOTE: Approximate FPGA IO Count = ~516
Ethernet Magjack
Ethernet PHY DP83865DVH 10/100/1000
30
DB9
RS232 MAX3221 CPWR
BOARD POWER CONN
POWER SUPPLY DISTRIBUTION
LED's
DEVICE PWR CONN
FET
+12V to all Devices
DSK PWR IN CONN
FET
DSK PWR OUT CONN
Used to sequence DSP DSK Board Power
32 Data
30 Addr & Ctl
DSP EMIF / EXP Connector (Samtec TFM-140 -32-S-D-LC)
LVDS Clock Pair
LVPECL Clock Pair
General Purpose DIP Switches
18 Control & Status
CLOCK Generation and Distribution
To DEV1, LVPECL Clock Pair
To DEV2, LVPECL Clock Pair
To DEV3, LVPECL Clock Pair
To DEV4, LVPECL Clock Pair
To DEV5, LVPECL Clock Pair
To DEV6, LVPECL Clock Pair
To DEV7, LVPECL Clock Pair
To DEV8, LVPECL Clock Pair
LVPECL AC CPL Clock Out
SMA CONN
LVPECL AC CPL Reference Out
SMA CONN
AC CPL Reference Input
SMA CONN
FPGA MODE SEL DIP SWITCHES
4
9
XCF32P x4 128 Mbits
REV-SEL[1:0], EN-EXT-SELn
JTAG CONN 2x7 (2mm)
3
FPGA REV SEL DIP SWITCH

Figure 7: MCDSP High-Level Block Diagram

The MCDSP architecture is shown in Figure 7. A list of major components used for the MCDSP is as follows:

Clocking:

- 10 MHz VCTCXO Internal Reference – FOX Electronics FOX801BELF-100
- RF Switch used for Clock Switching - Analog Devices ADG918BRM
- External Clock Input LVPECL Fanout Buffer – Micrel SY100EP11UZI/KI
- Wide Band Low Jitter Clock Source – Analog Devices ADF4350BCPZ
- Clock Distribution and Optional VCXO Based PLL – Analog Devices AD9511BCPZ
- Clock Distribution to Devices – National LMK01020ISQE

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

Power:

- 1.0V DC/DC Converter – Texas Instruments – PTH04T231W
- 1.8V DC/DC Converter – Enpirion – EN5336QI
- 2.5V DC/DC Converter – Enpirion – EN5336QI
- 3.3V DC/DC Converter – Enpirion – EN5322QI
- 3.7V DC/DC Converter – Enpirion – EN5336QI
- Clocking LDO's – Texas Instruments – TPS78633DCQ
- PLL VCO LDO – Texas Instruments TPS79333DBV
- VCXO LDO – Texas Instruments TPS79333DBV
- TCXO LDO – Texas Instruments TPS79330DBV
- GTP LDO's – Texas Instruments – TPS74801DRCR

Miscellaneous:

- FPGA – XILINX XC5VSX95T-1FFG1136C
- FPGA Programming PROM (x4) – Xilinx XCF32PFSG48C
- RS232 Transceiver – Maxim MAX3221CPWR
- Ethernet PHY – National DP83865DVH
- 200 MHz XO for DDR Calibration and Misc – Crystek CCPD-034-50-200.000
- 156.25 MHz Rocket IO Clock Reference – Crystek CCPD-033-50-156.250
- 64M x 16 DDR – Micron MT47H64M16HR-3
- Device Connectors – Samtec QSH-040-01-F-D-DP-A
- Rocket IO Connectors – Molex 73412-0110 (UFL)
- Rocket IO Cable Assembly – Samtec MH113-MH1RP-01BJ1-0150 (UFL to SMA-F)
- DSP Processor Board interface Connector – Samtec TFM-140-32-S-D-LC
- FPGA JTAG Connector – Molex 87832-1420

2.1.2 Functional Overview of MCDSP Hardware

- Main power is 5V and is connected to a 2.1mm barrel type connector (J4). Main power is turned on and off using toggle switch (SW3). Power for the DSP Processor board should be routed through the MCDSP to allow for power sequencing control by the MCDSP. The power input should be 5V and supplied to the 2.1mm barrel connector (J3). The sequenced output is on the 2.1mm barrel connector (J1). This is done so that the FPGA IO's can be protected. The 8 device connector's power should be supplied on the 2.1mm barrel connector (J11). Power to the 8 device connectors is also sequenced on the MCDSP board. Device power MUST be supplied.
- The DSP Processor connection on the MCDSP interfaces to the Xilinx FPGA via a 32-bit wide bus and an addition 30 address and control lines.
- The MCDSP includes user defined FPGA LEDs and 8 DIP switches.
- The 8 device connectors allow the connection of high speed ADC's or DAC's. The interconnection to the FPGA, for each device, is via 16 bit wide LVDS pairs. In the case of the ADC's, an LVDS pair is routed back to the FPGA clock pin. This allows the use of the ADC clock output. Additional SPI controls and device ID connections are also provided.
- Two Rocket IO transceiver pairs are provided on SMA connectors.

- JTAG Interface for the FPGA allows the user to configure the FPGA with user specific FPGA code and is accessible via Connector J2. Up to 4 revisions can be selected using the revision dip switch SW1.
- A Tri-mode Ethernet and RS232 interface is directly connected to the FPGA.
- Flexible low jitter clock generation and distribution is provided to the FPGA and all 8 device daughter card connectors. The PLL based clock generation and distribution can support clocks from 1MHz to 1GHz. An optional VCXO implementation can be supported. The clocking divide ratio and delay can be manipulated for each clock output. An internal low noise TCVCXO provides a 10 MHz reference. An external reference can be supported (1MHz to 105MHz for PLL based and up to 200MHz for VCXO based). The external reference input is via a 50 Ohm SMA connection (J20). The internal or external reference is provided as an output on an SMA connector (J18). A clock up to 1GHz can be routed to the external clock output SMA connector (J12).

2.1.3 Clock Synthesizer

The clock synthesizer (shown in Figure 8) design is extremely crucial as the phase-noise and jitter specifications of the on-board clocks will ultimately influence the synthesized waveform performance. The clock synthesizer consists of the following major components:

- **10 MHz VCTCXO Internal Reference – FOX Electronics FOX801BELF-100**

Used as on-board high stability reference. This clock reference has ±2.5PPM stability at 1Vpp output.

- **RF Switch used for Clock Switching - Analog Devices ADG918BRM**

This switch selects an external 10 MHz reference input or the on-board 10 MHz VCTCXO. The control is provided by the FPGA, and the default configuration is selecting the on-board clock reference. This switching provides an option to synchronize the MCDSP to an external source (generated from another MCDSP or any other circuit).

- **External Clock Input LVPECL Fan-out Buffer - Micrel SY100EP11UZI/KI**

This device is used to fan-out the reference 10 MHz clock to the PLL section and to an on-board SMA (for use as a synchronization clock reference to other circuits).

- **Wide Band Low Jitter Clock Source – Analog Devices ADF4350**

This is the main PLL with an integrated wideband VCO.

- **Clock Distribution and Optional VCXO Based PLL – Analog Devices AD9511**

This is an optional PLL which can phase-lock an external low-jitter VCXO to the 10 MHz reference clock. This PLL can be used for jitter specific applications where dynamic clock adjustment is not necessary. In all other cases, where the ADF4350 is the main PLL, the AD9511 can be used only for clock distribution and pre-scaling.

- **Clock Distribution to Devices – National LMK01020**

This provides 1:8 clock distributions for the synthesized clock up to 1.2 GHz, which is routed to each of the device connectors. Along with clock distribution, this device provides clock division and clock skew adjustment (150ps step) for each of the buffered LVPECL clock.

The complete block diagram of the clock synthesizer section is shown below.

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

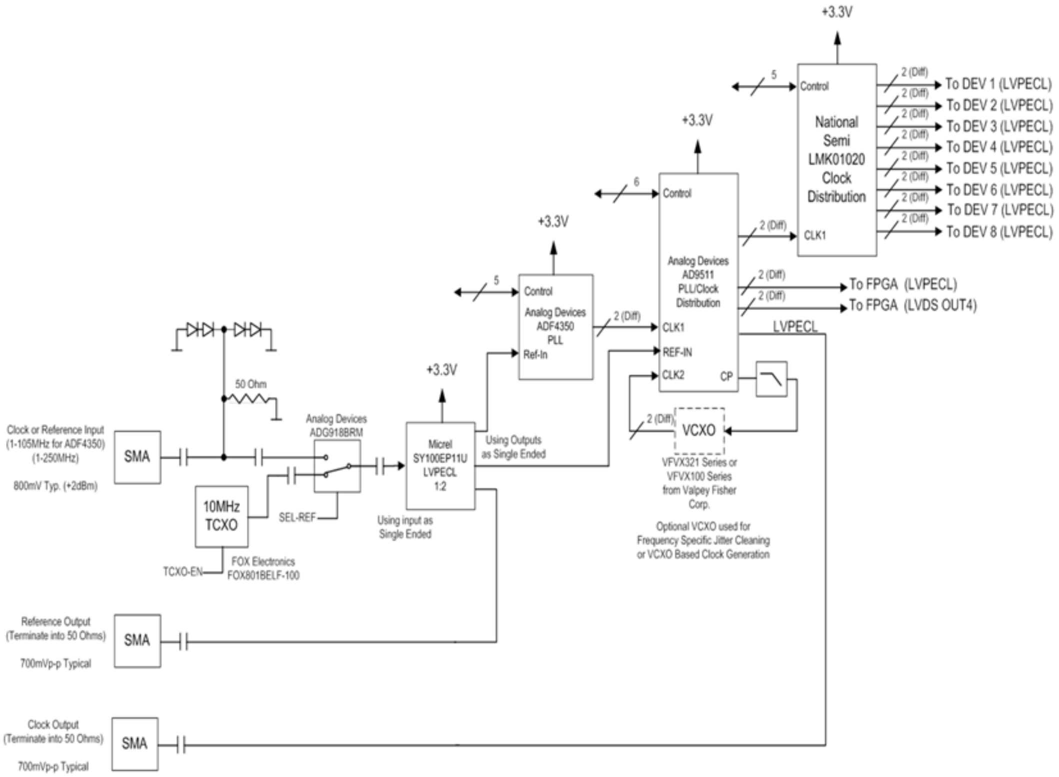


Figure 8: The MCDSP Clock synthesizer block diagram

A detailed system clocking block diagram is shown in below.

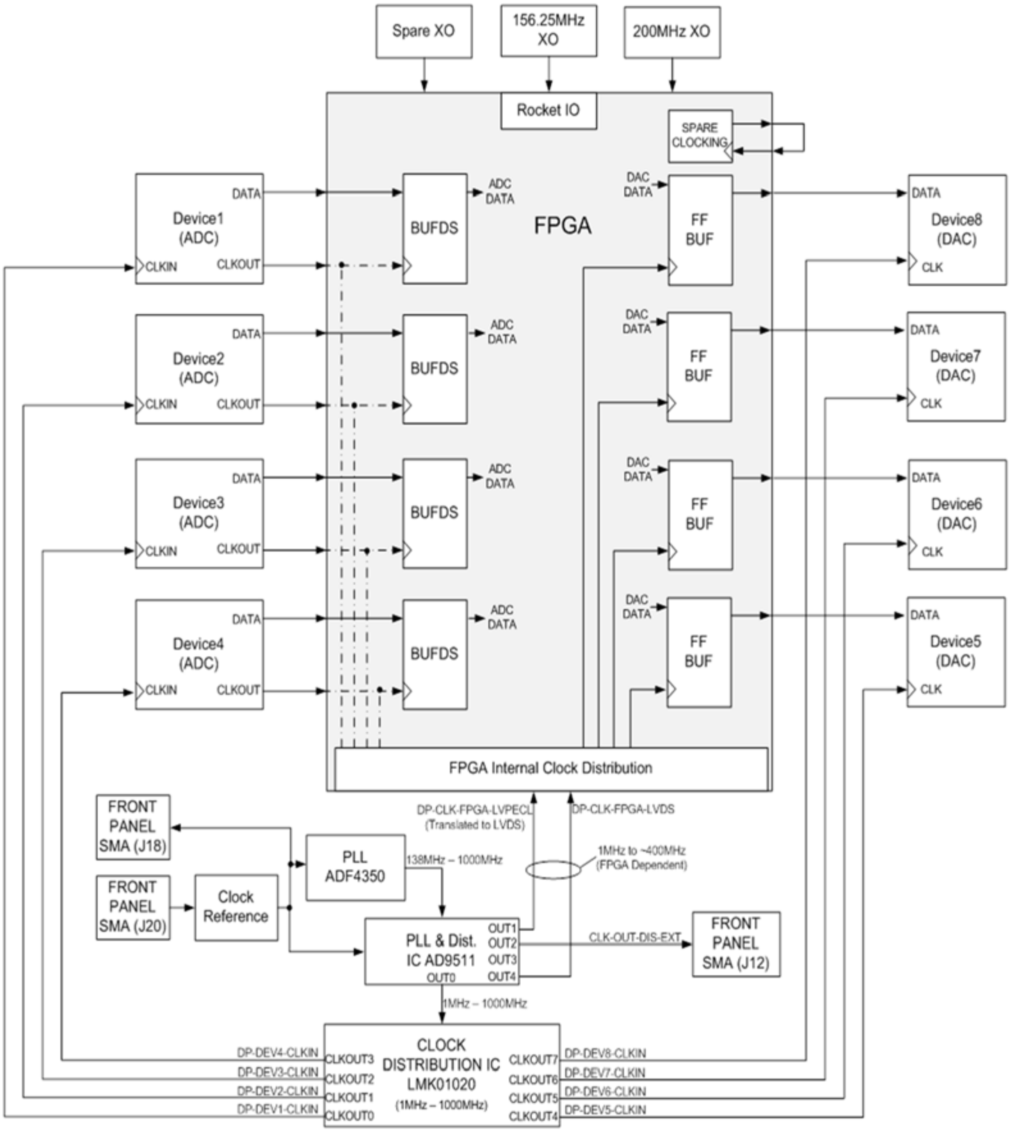


Figure 9: MCDSP System Clocking Block Diagram

The Figure 9 shows a typical configuration with 4-D/A converters or transmitter channels and 4 A/D converters or receiver channels. But any configuration can be decided by the user. One MCDSP module can act as a dedicated multi-channel transmitter and another MCDSP as a dedicated multi-channel receiver. These modules can be phase synchronized with each other.

2.1.4 Power Supply

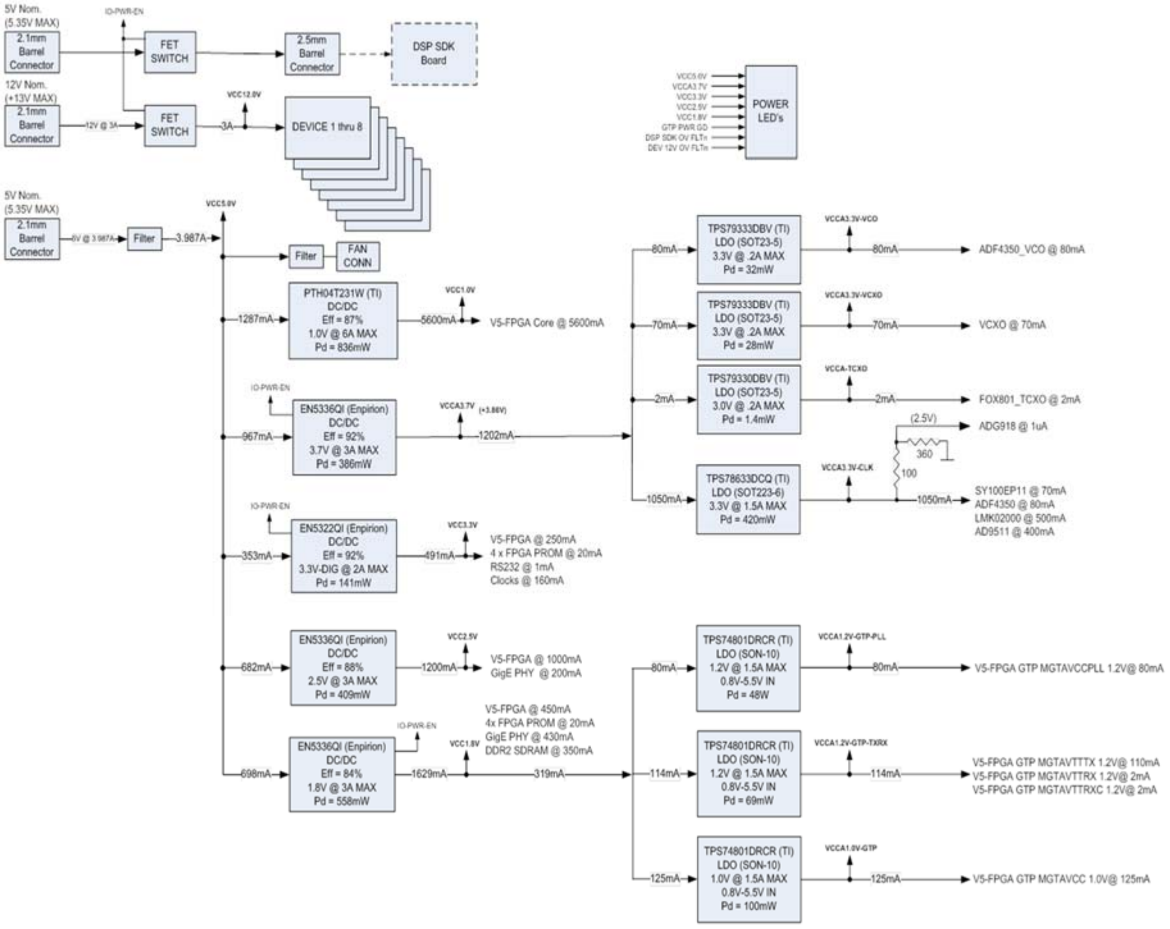


Figure 10: Power supply components on the MCDSP and their interconnections

The **Figure 10** shows the power supply connections on-board. The design has been kept very conservative to support a wide range of FPGA devices in the Virtex-5 Family. The power supply design can support a 5V DC input and draw a maximum of 4 Amp current (20Watt). Separate power supply inputs are provided for an external DSP board and RF devices for safety. The necessary power conditioning and DC barrel connectors are already provided on board. The MCDSP takes a 5V +/- 5% DC at the input power connector and on-board regulators generate 5V, 1V, 3.7V, 3.3V, 2.5V, 1.8V outputs, which are correctly sequenced

2.1.5 MCDSP Plug-in Devices

The Figure 11 shows how multiple device cards can be plugged on-to the MCDSP board. A typical device card is typically 3' x 1.75" with each card supporting 1 to 4 channels, depending on the processed bandwidth. The bandwidth is controlled either by driving the 16 bit differential data interface at full speed (highest bandwidth) or by time-interleaving multiple channel information on the single data stream (few 10's of MHz bandwidth). The DSP-SDK board is optional and represents a floating point DSP processor communicating with FPGA via the Extended Memory Interface (EMIF).

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

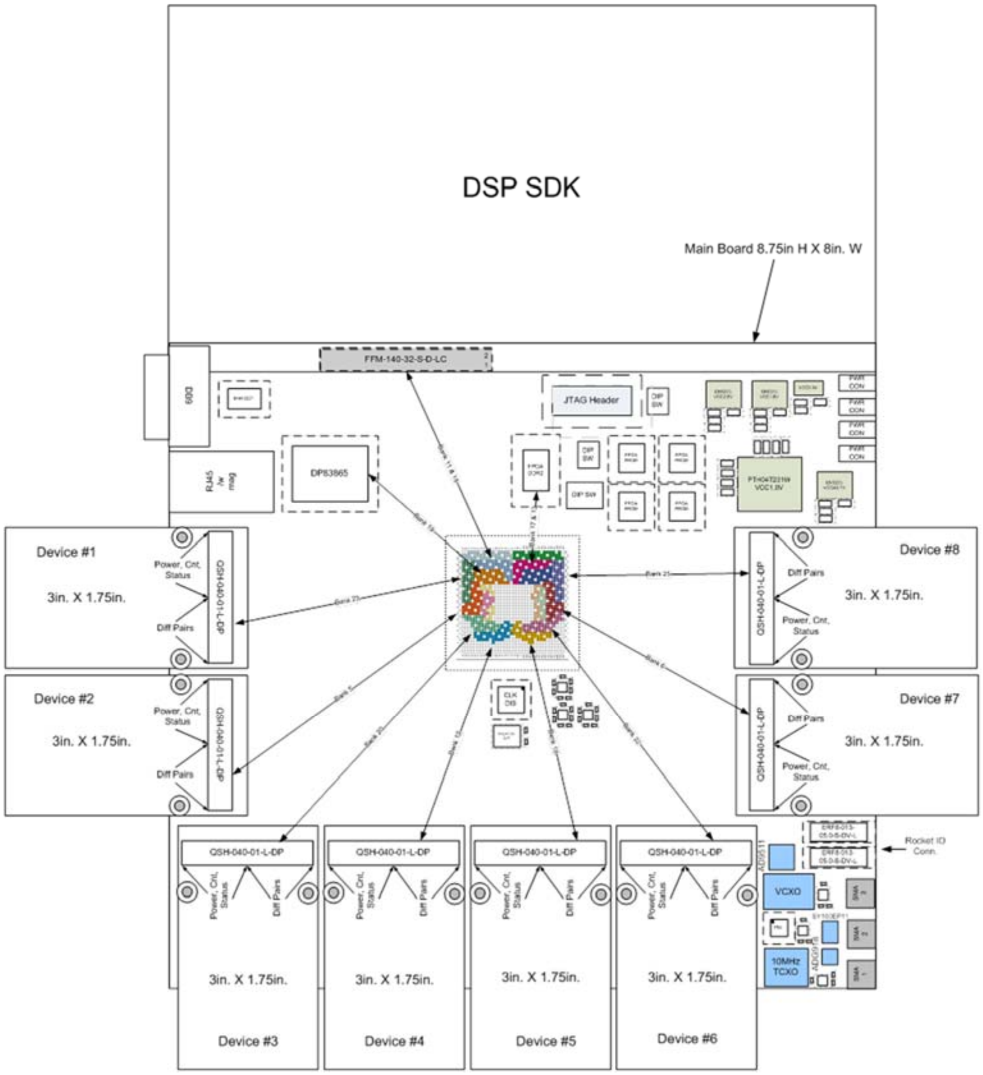


Figure 11: MCDSP with plug-in device cards and a DSP processor interface

2.2 Cellphone Detection FPGA Firmware Architecture

The FPGA firmware consists of a digital down-conversion (DDC) stage. The LO signal for this DDC is fixed at 71.7MHz for 850MHz receivers. This LO signals is generated within the FPGA from a Numerically Controlled Oscillator (NCO). This DDC implementation lowers the IF range of 74-99 MHz to 2.3- 27.3 MHz. The sampling rate is decimated by 4. Thus the cellphone spectrum is now digitally represented from 2.3-27.3 MHz sampled at 62.5 MHz (250 MHz decimated by 4).

This down-sampled data is constantly monitored by an energy detection module implemented on the FPGA. This module performs averaged Fast Fourier Transform (FFT) of the four received signals in a parallel pipelined fashion. The user has to input the desired cellular channel to be monitored for activity. The frequency bin value of the averaged FFT corresponding to the desired cellular channel is compared to the receiver noise (initial 1 MHz or trailing 1MHz of the FFT output, as no channel activity is expected here). If the FFT value is greater than the receiver noise by a user-defined threshold, then a “signal-detect” indication is generated. This prompts the data

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

acquisition controller within the FPGA to store 32K samples of the received cell-phone signal, per channel. This stored data is downloaded to a PC using 1-Gigabit Ethernet link from the FPGA. The Ethernet MAC and Packetizing modules are also implemented on the FPGA.

2.3 RF Receiver Front End

A block diagram of the front end is shown in and the board for one channel is shown in Figure 12 and Figure 13. Four of these were used for the project, one for each antenna. Modifications made for the NIJ projects include the addition of the Epcos 836MHz band pass filter and the bypassing of the original ceramic filter and use of an SMA connectorized 836MHz band pass filter. The transfer function of these filters is shown in Figure 14 and Figure 15.

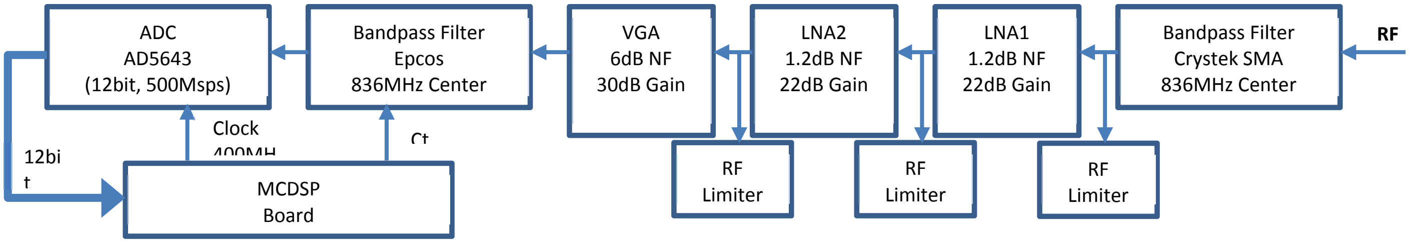


Figure 12: Block diagram of a single RF channel on the plug-in direct digital receiver

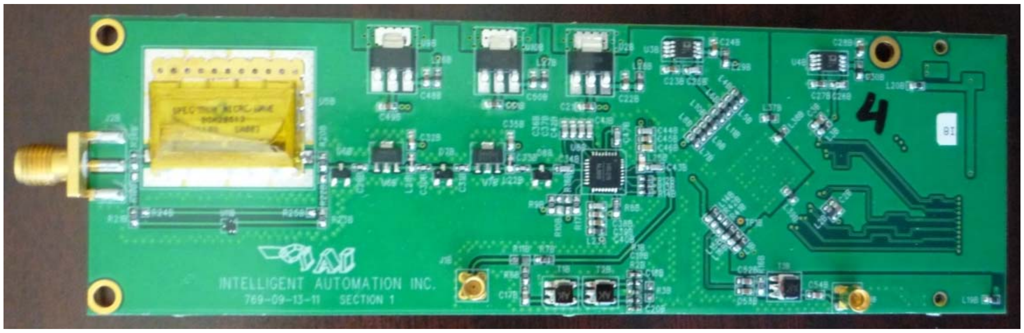


Figure 13: RF front end, single channel

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

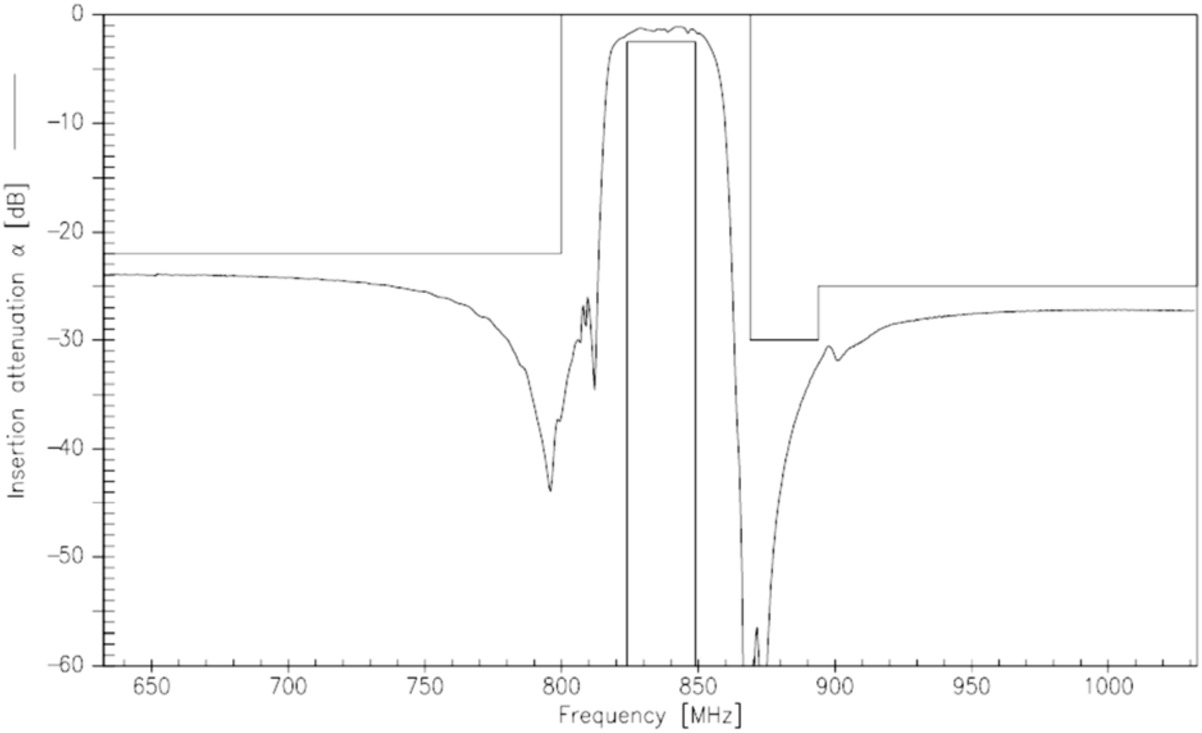


Figure 14:Transfer function of additional bandpass filter added to RF front end board to help detection performance of weak cell phone signals. Center frequency at 836MHz.

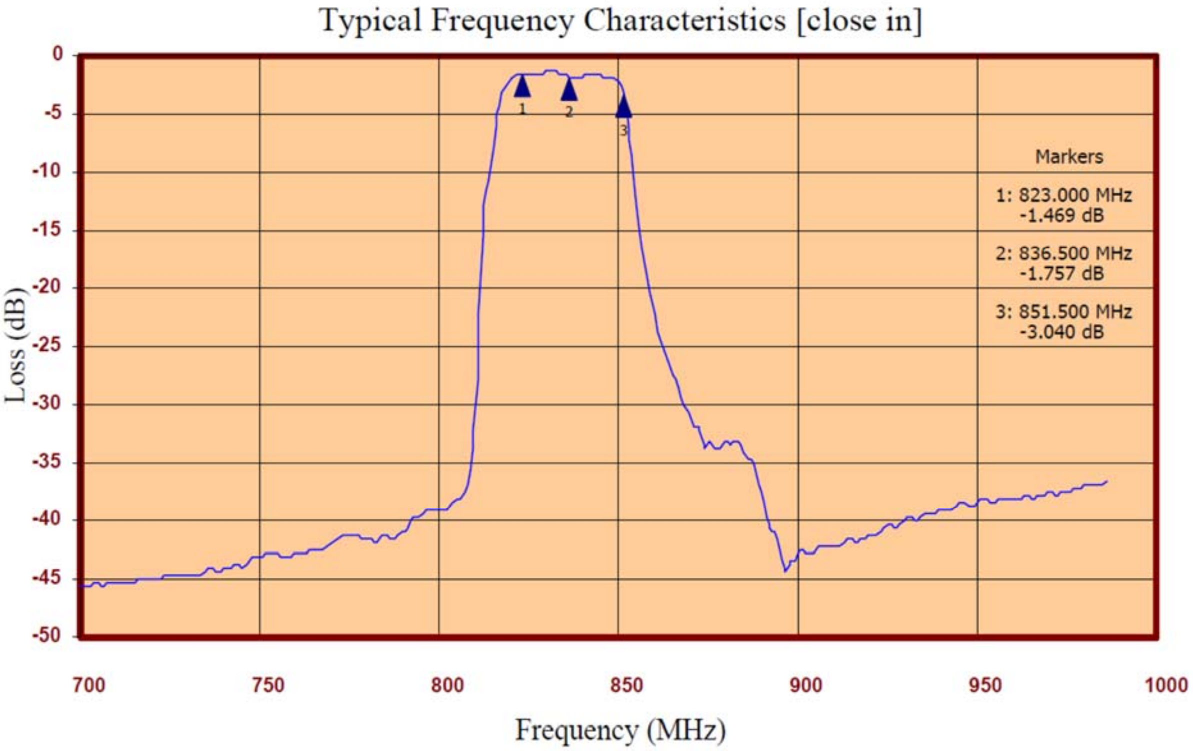


Figure 15: Spectrum of Crystek band pass filter, center frequency 836MHz

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

2.3.1 Sampling Rates

The sampling rate of the ADCs is 250MHz. The aliasing bands are 0-250, 250-500, 500-750, 750-1000MHz, etc. We are interested in the seventh Nyquist zone of 750-875MHz. With the use of two 824.2-849.2MHz band pass filters, we effectively block out any signals that appear outside of this seventh Nyquist zone. The cell phone signal thus shows up at 74.2-99.2MHz. The FPGA down converts using 73.2MHz, which results in frequencies of 1-26MHz. To increase the number of points that are stored in memory, the signal is decimated by four which results in an effective sample rate of 62.5MHz, which is greater than twice 26MHz.

Note that with modified receiver boards, the MCDSP can accommodate a total of 16 antennas. It could also be useful for buildings such as those at the Lawrenceville facility that may require a set of four antennas per zone. This could be useful if it's decided it is necessary to use multiple antennas per location to add an angle of arrival approach to locating cell phones.

2.3.2 RF BPF

A high-rejection band-pass filter is essential at the front-end following the antenna to reject out-of-band noise. The Crystek CBPFS-0836 SAW filter is used for this application.

2.3.3 LNA-1

The RF LNA provides roughly 24 dB gain in the 824-849 MHz band at low noise figure (1.2 dB typical). The Triquint TQP3M9009 RF evaluation board is used here.

2.3.4 LO Generator

An RF signal generator is used to generate the 750 MHZ LO signal. IAI has two signal generators capable of generating this signal (HP-8648C and the HP-8656B). The output level is set at 6dBm.

2.3.5 RF Splitter (1:4)

A passive RF splitter is used to split the 750 MHz LO signal generated from the signal generator. The 6dBm output from the Signal generator suffers roughly 8dB attenuation from the splitter / channel. The resulting -2dBm LO signal at 750 MHz is sufficient to drive the active RF mixer.

2.3.6 RF Mixer

An active single sideband mixer is used to down-convert the 824-849 MHz Cellular RF to IF range. The Linear Tech LT5522 evaluation board is used for this application.

2.3.7 IF BPF

The IF BPF filters out the 74-99 MHz IF band after analog down-conversion. The Minicircuits SXBP-100 is used here.

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

2.3.8 LNA-2

The LN provides additional 23 dB gain at the IF frequency of 74-99 MHz. the LNA-580 from www.rfbayinc.com is used here.

2.3.9 IF LPF

The IF LPF provides further out-of Nyquist noise rejection before the IF signal is provided to an ADC. The Minicircuits SX75LP-105-S+ is used here.

2.3.10 ADC

The AD module is designed as a plug-in card for the MCDSP. The primary ADC is a dual-channel LTC2158-14 ADC from Linear-Tech. the maximum sampling rate is 310MHz at a resolution of 14-bits. Two plug-in ADC cards are used to cover simultaneous sampling for 4-channels at 250MHz each.

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

3. Cell Phone Signal Transmitter

3.1 CDMA2000 Modem Working on Verizon Network

At the beginning of the data collection and experiments, a CDMA2000 modem is used to transmit cell phone signals, shown in **Figure 16**. At the transmitter end of the system, the cellular modem is programed by an accompanying laptop to send out text messages repetitively with a controlled delay between two consecutive transmissions. One advantage of using a modem instead of a cell phone is the transmissions are more repeatable, since the tester does not have to handle the modem during testing which inevitably results in RF variations to due to varying holding angles and antenna blockages. Another advantage of using a cellular modem lies in the fact that it has a SMA connector to allow for direct wired hook-up to the signal receiving hardware; this is very useful for controlled testing and calibration for the difference between cable lengths.

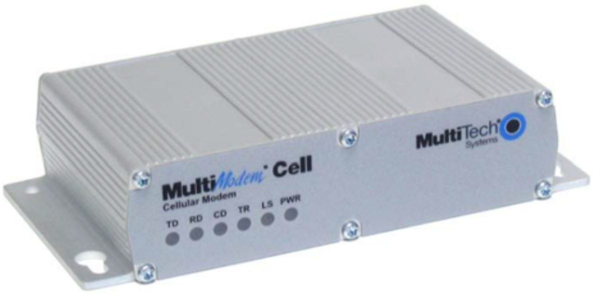


Figure 16: CDMA2000 modem used as the transmitter for testing

3.2 Verizon Cell Phone

For demonstration purposes, we decided to use cell phone for data collection and experiments. A Verizon prepaid CDMA2000 cell phone is acquired and used in the data collection and later experiments, which is shown in the middle of Figure 17. It is operating in 850MHz band. The cell phone is running on an Android system, which allows us to program the cell phone to send out text messages in a regular manner.

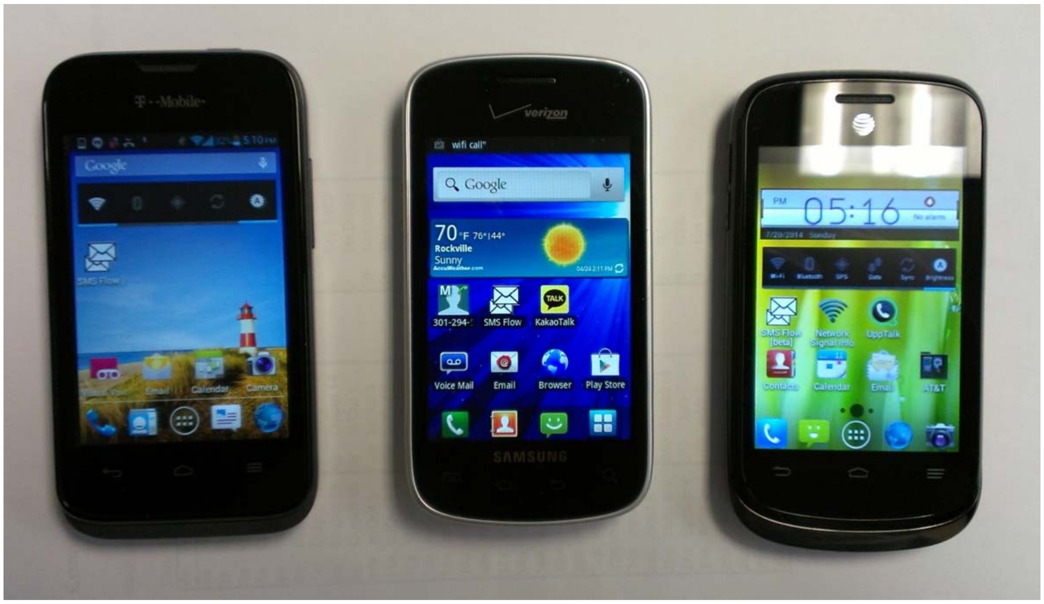


Figure 17: Prepaid cell phones from Verizon, AT&T and T-Mobile

3.3 AT&T Cell Phone

A AT&T prepaid cell phone is acquired (the right one shown in Figure 17) and used in the data collection and later experiments. It is running on AT&T 3G networks, which is primarily 1900MHz WCDMA network in the experiment area. It can also be programmed to send regular text messages for this testing purpose.

3.4 T-Mobile Cell Phone

A T-Mobile 3G prepaid cell phone (the left one shown in Figure 17) is acquired and used in the data collection and later experiments. This cell phone is operating at 1700MHz in both GSM and WCDMA network. It can also be programmed to send regular text messages for this testing purpose.

4. Signal Processing and Algorithm Development

4.1 A Brief Introduction to Data Collection and Pre-processing of Data

A typical RF transmission from a cell phone results in four received signals, at the four different channels of the receiver. The received signals can alternatively be viewed as a time series of voltages. Although the exact time series varies over time because of pseudo-randomness of the CDMA code, it is legitimate to expect that the correlation function has temporal stability near the primary lobe.

In the fingerprinting based approach we have to extract some parameters, known as features, for characterizing a point. This features should satisfy two important properties, namely they should be sensitive to spatial displacement but at the same time quite stable with respect to temporal displacement. For this particular problem, we choose as the features to consider: a) the signal strengths at four different signals and b) the time difference of arrival (TDOA) at antenna number 1, 2 and 4 with respect to the antenna at location 3.The computation of signal strength is straight-forward because it is defined as the absolute mean of the received voltages. But to get the TDOA between two received signals we have to find out the correlation peak between them. The next subsection provides a brief description of that step.

4.2 Determination of time difference between received signals

First, the received signals go through a 100th order software band-pass filter to isolate the channels of interest – this is performed for testing convenience to filter out GSM or other signals that occasionally show up lower in the 800MHz band. It is difficult to find an accurate peak of this correlation function because it is both signal and negative and is not yet down converted. Down conversion is not used because the channel which 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 its exact value by low pass filtering the square of the correlated signal. The correlation must be squared in order to present a DC component to the low pass filter. A sharp 400th 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-nanosecond 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.

4.3 Tests to characterize the environment without active transmissions

We performed tests to characterize the environment without active transmissions during late evening ours, during which time nobody was in the IAI offices and no cell phone were used in the office. In this test, the cellular modem is left on without any scheduled transmission, and the receiving circuit was kept on. In the experiment conducted on 06/12/2012, we obtained 662 receptions and out of these 662 receptions 131 (~20%) were within the frequency band of our interest, i.e. between CDMA2000 channel number 490 and 530. We tried to find the source location of these 131 transmissions. Almost all localization approaches identified the most probable room as the room where the modem was placed. On 06/28/2012 night, we performed the no transmission test again, but with the modem totally powered off and the receiving circuit kept in operation. Under this condition, almost no signals were received.

Through these no transmission tests and comparisons, we figured out that the modem or cell phone talks to the base station periodically as long as it is powered on, but there is no environmental interference signal in the CDMA2000 bandwidth. Thus, these experiments confirmed our assumption regarding RF quietness in our building (within the frequency band of our interest) during off hours.

4.4 Variation of Features across Different Channels

One of the desired properties of the features is stability across different CDMA channels because, in the practical scenario, a priori information about the CDMA channel will not be available. Therefore, we studied the variation of the features, namely signal strengths and TDOAs, for all test locations. Our primary observations were: a) the signal strengths become more sensitive to the channel number as we move away from the receiver and b) the TDOAs are less sensitive to the variation of the channel being used.

Support of these observations is as follows. Figure 18 through Figure 21 show the variation of the signal strength (i.e. absolute mean) and the TDOA of the signal received at antennas 1-4 across different channels for the set of data collected at location number #50. In the number of occurrences plots, the instances where the signal is received at some channel outside the normally received band of channels (490-530) are marked in red. As the antenna 3 is being used as reference for TDOA computation, Figure 20 shows the zero value for TDOA at antenna 3, as expected. The existence of outliers is indicated by red colored plus signs. One note is that the modem only uses our channels for transmission, the wide various in channels in the below plots are the algorithm’s calculation of transmitter channel which can be imprecise at low SNRs.

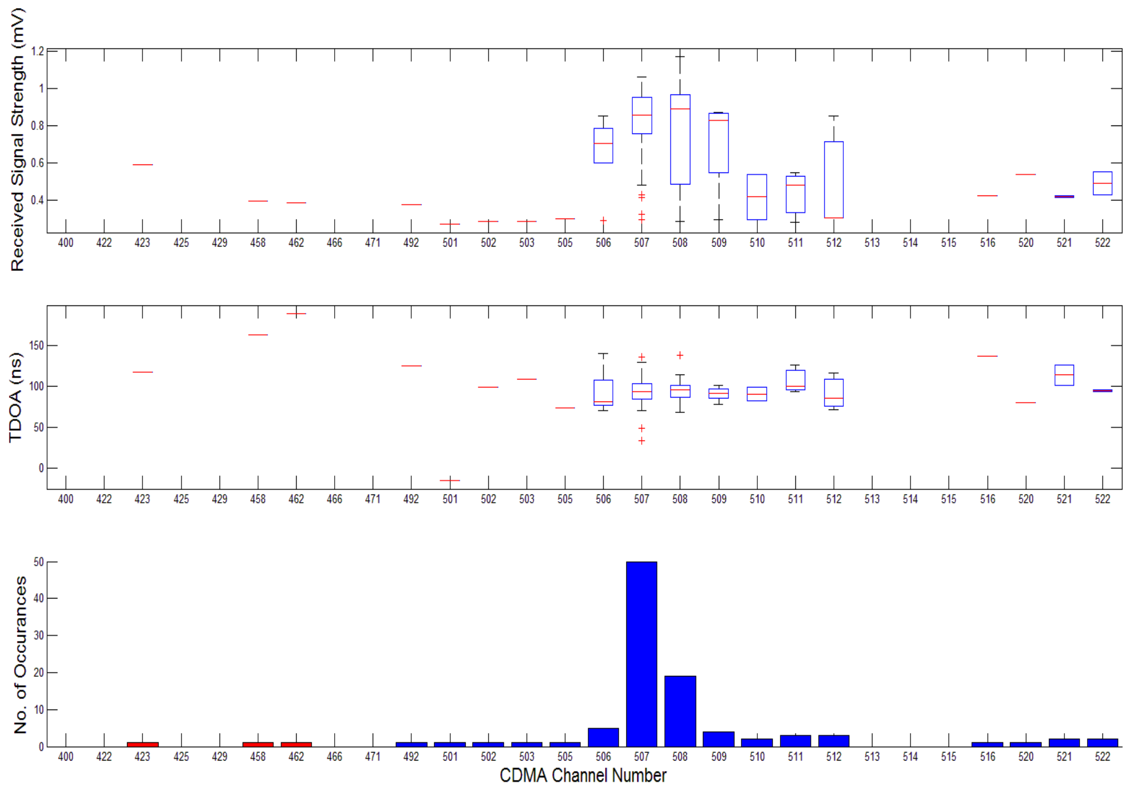


Figure 18: Variation in strength and TDOA of the signal received at Antenna 1.

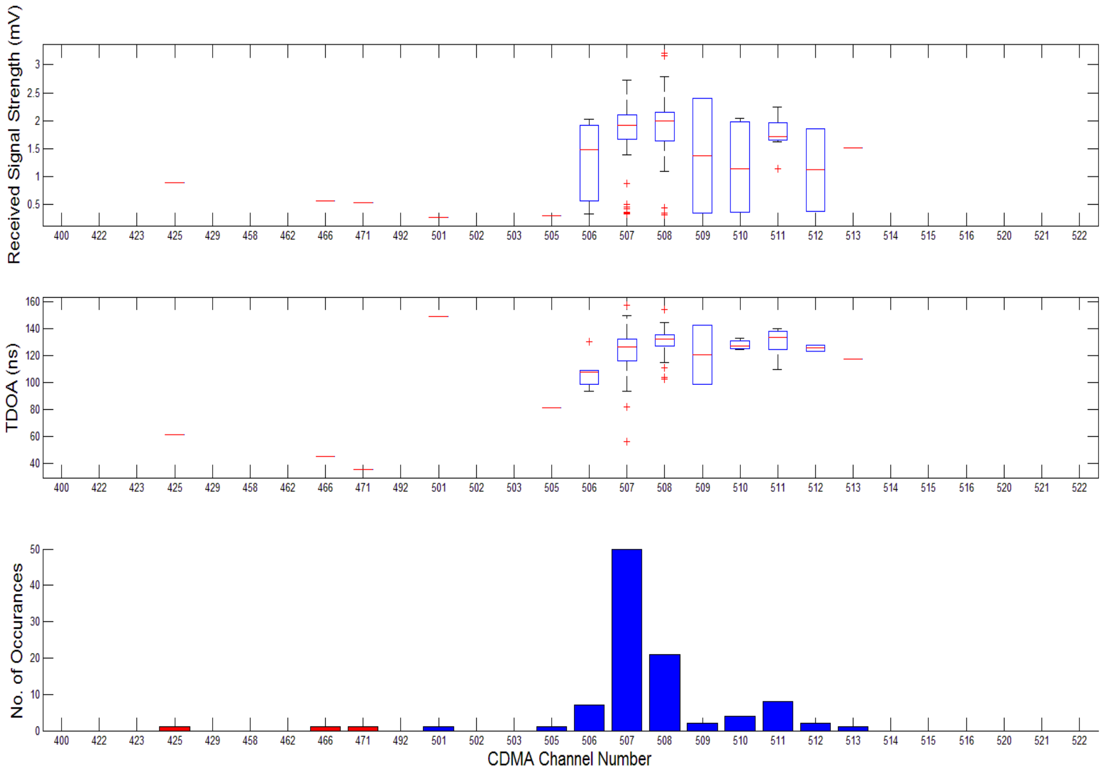


Figure 19: Variation in strength and TDOA of the signal received at Antenna 2

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

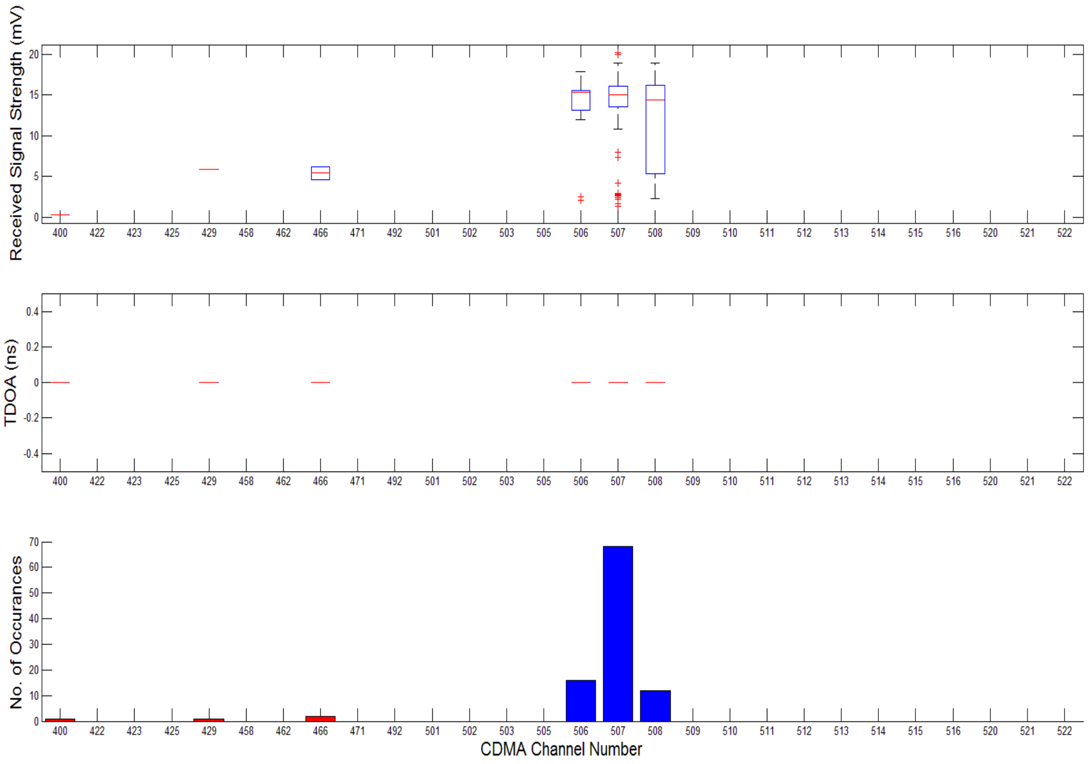


Figure 20: Variation in strength and TDOA of the signal received at Antenna 3

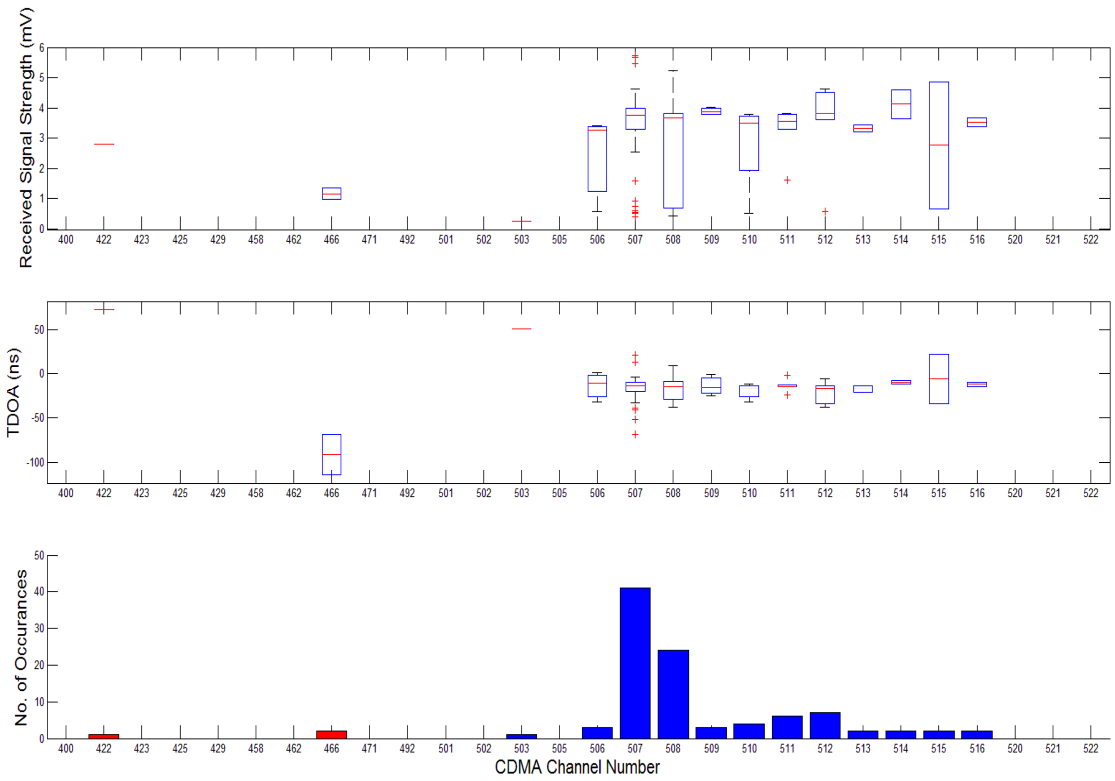


Figure 21: Variation in strength and TDOA of the signal received at antenna 4

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

4.5 Removal of Outliers

Before the start of analysis, we decided to remove some outliers, although the criteria for classifying a reception as an outlier are based on heuristics to some extent. The outlier removal process takes place in two steps:

- We throw away any observation if any of the four receiving antennas gets the transmission outside the frequency band of our interest, i.e. CDMA2000 channels in the 490-530 range. Note the channels the modem uses to use is not under our control, it is directed to the modem by the cellular tower.
- Once we have thrown away the outliers based on the channel information, we compute the mean (μ_l^i) and standard deviation $(\sigma_l^i)$of a particular feature "i" obtained from a particular location"l". Then we throw away all the observations where either of the seven feature values lies outside the $(\mu_l^i \pm 3\sigma_l^i)$ region.

This two-step outlier rejection process gives us a refined data set and removes around 13% of the collected data as outliers.

4.6 Data Set Classification

Once we have gathered the data, free from outliers, we use MATLAB to achieve the classification goal. The statistics toolbox of MATLAB contains a command called *classify* which can classify a set of test data, given a set of training data along with the associated labels. This function has five different options to choose the classification algorithm, default being the *linear*. All but one approach solves the classification by maximizing the posterior probability. As the posterior probability can be represented as

$$P[class|feature] = \frac{P[feature|class]P[class]}{P[feature]}$$

After the classification, we need the prior distribution and the conditional distribution of the feature as a starting point. MATLAB assumes multivariate Gaussian to be underlying conditional distribution and unless it is stated otherwise, the uniform distribution, i.e., $\pi_k = \frac{1}{M}$ for all the classes, is assumed to be the default choice for prior distribution.

4.6.1 Linear Discriminant Analysis (*linear*)

This algorithm approaches the problem by assuming normality on the distribution of features from a particular class, or in other words, it assumes that the distribution of features (f_i) from a particular class "i" is a multivariate Gaussian. Moreover it assumes equality of the covariance matrices.

Suppose there are M classes in total and the i^{th}-class has an empirical mean of μ_i. Let, Σ be the empirical covariance, stratified by the sample size and the number of groups, i.e.,

$$\Sigma = \frac{1}{\sqrt{N-M}} \sum_{i=1}^{N} (x_i - \mu_k)(x_i - \mu_k)^T$$

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

where, the observed feature x_i belongs to the class $C = k$. Then $f_i \sim \mathcal{N}(\mu_i, \Sigma)$ and we classify an unlabeled feature "x" by solving the following maximization problem

$$\begin{aligned}
\underset{k \in \{1, \cdots, M\}}{\operatorname{argmax}} f(C = k|x) &= \underset{k \in \{1, \cdots, M\}}{\operatorname{argmax}} \frac{f(x|C = k)P[C = k]}{f(x)} \\
&= \underset{k \in \{1, \cdots, M\}}{\operatorname{argmax}} \big(\log P[C = k] + \log f_k(x) \big) \\
&= \underset{k \in \{1, \cdots, M\}}{\operatorname{argmax}} \big(\log \pi_k - \frac{1}{2} \log |\Sigma| - \frac{1}{2}(x - \mu_k)^T \Sigma^{-1} (x - \mu_k) \big) \\
&= \underset{k \in \{1, \cdots, M\}}{\operatorname{argmax}} \big(\log \pi_k - \frac{1}{2}(x - \mu_k)^T \Sigma^{-1} (x - \mu_k) \big).
\end{aligned}$$

4.6.2 Linear Analysis with an Extra Assumption of Independence (diaglinear)

This is special case of the linear analysis, where an extra extra assumption is made on the structure of the covariance matrix Σ. We assume the covariance matrix to be a diagonal one, i.e. we assume independence between different parameters of the observed variables.

4.6.3 Quadratic Discriminant Analysis (quadratic)

This method allows a room for variation in covariance between different classes. Everything else remains the same compared to the linear analysis. Therefore, this algorithm solves:

$$\underset{k \in \{1, \cdots, M\}}{\operatorname{argmax}} \big(\log \pi_k - \frac{1}{2} \log |\Sigma_k| - \frac{1}{2}(x - \mu_k)^T \Sigma_k^{-1} (x - \mu_k) \big)$$

where Σ_k is the empirical covariance of the k^{th}-class, stratified by the number of elements belonging to that class.

4.6.4 Quadratic Analysis with an Extra Assumption of Independence(diagquadratic)

The difference between diagquadratic and quadratic is same to the one between diaglinear and linear, i.e. this is a special case of quadratic where independence is assumed between different parameters of the observed variables.

4.6.5 Analysis Based on Mahalanobis Distance (mahalanobis)

This algorithm associates each class k, with an empirical class mean μ_k and a class stratified covariance matrix Σ_k. Then it classify an unlabeled sample, by finding its closest class mean (μ_k) with respect to the Mahalanobis distance, or in other words, this approach solves the classification problem through the following optimization

$$\underset{k \in \{1, \cdots, M\}}{\operatorname{argmin}} \sqrt{(x - \mu_k)^T \Sigma_k^{-1} (x - \mu_k)}.$$

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

This approach is distinct from the other four approaches because this one doesn't try to maximize the posterior probability.

4.6.6 Support Vector Machine (SVM) classifier

This method uses SVM with Radial base function (Gaussian) kernel. First, binary classification between each room and the rest of the rooms is performed. The data is classified to the room with the highest posterior distribution. The package "libsvm", available from http://www.csie.ntu.edu.tw/~cjlin/libsvm is used. Training, using the available data with cross-validation is implemented to determine optimal the range of parameters.

4.7 Results Obtained Using classify

For the problem of our consideration, the features lie in $\mathbb{R}^7$, namely:

1. Signal strength at antenna # 1
2. Signal strength at antenna # 2
3. Signal strength at antenna # 3
4. Signal strength at antenna # 4
5. TDOA at antenna # 1 w.r.t. antenna # 3
6. TDOA at antenna # 2 w.r.t. antenna # 3
7. TDOA at antenna # 4 w.r.t. antenna # 3

and their associated class is given by the particular room from where the data was collected. We have a class of 10 members. To test our algorithm in a more realistic manner, the refined data set has been divided into the training and test data set in such way that there is no training data from a particular test location while we test the classification algorithm on the data collected from that location. This gives us a pessimistic estimate about the performance of the classification algorithm. After we have classified each of the multiple observations taken from particular test location, the success rate is computed. We have used two different notions of success, *original* and *relaxed*. A classification is successful in an *original* sense when the most likely room is same as the ground truth. And a classification is called to be successful in a *relaxed* sense if the following conditions hold true:

- the room with highest posterior probability is a neighbor of the ground truth, and,
- the ground truth has the second highest posterior probability.

The inbuilt *classify* routine doesn't give the distribution of posterior probability while performing classification by minimizing the Mahalanobis distance between the unlabeled sample and the empirical class mean. Therefore the relaxed sense of success is not valid when we use "*mahalanobis*" as the method-type.

Success rate (at a particular test location) is defined as the ratio of the number of successful classifications to total number of transmissions made from that particular test location. Figure 22 to Figure 26 show the variation in *success rate* (in both original and relaxed sense) across different test locations (plotted along x-axis). Success rate below 75% are represented by a red bar. Visual comparison between Figure 22 and Figure 23 helps to conclude (in a qualitative way) that *diaglinear* yields a worse result than that produced by the *linear* method. A similar conclusion can be drawn by comparing Figure 24 and Figure 25. On the other hand, overall superiority of *quadratic* over *linear* can be inferred from Figure 22 and Figure 24.

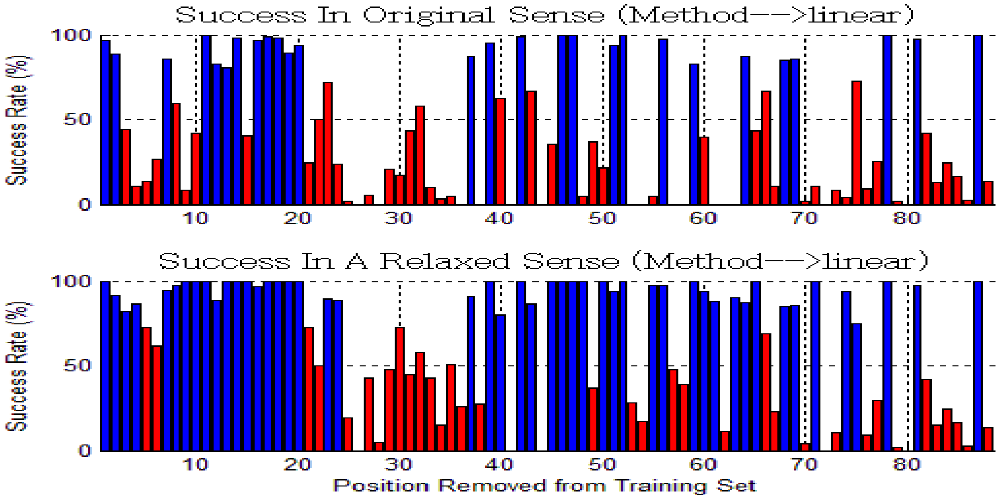


Figure 22: Success rate in classifying data obtained from different test locations (*linear*).

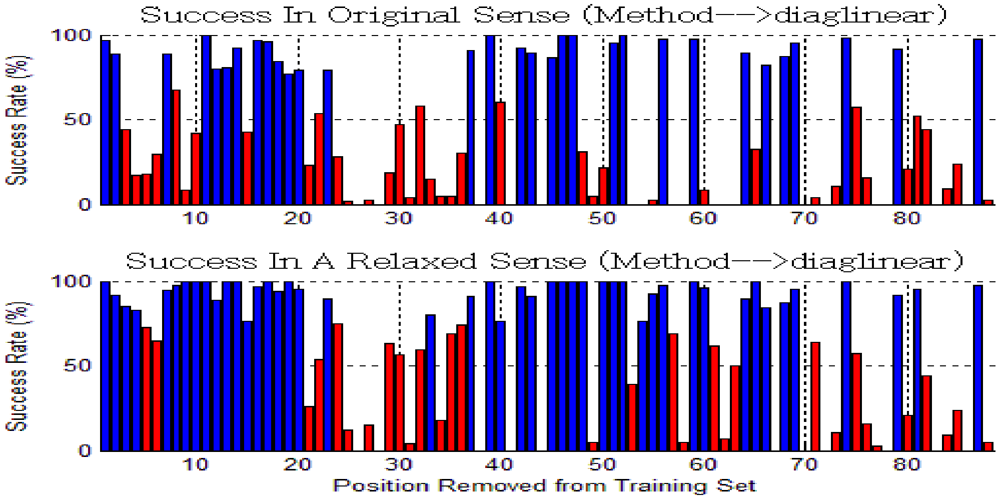


Figure 23: Success rate in classifying data obtained from different test locations (*diaglinear*).

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

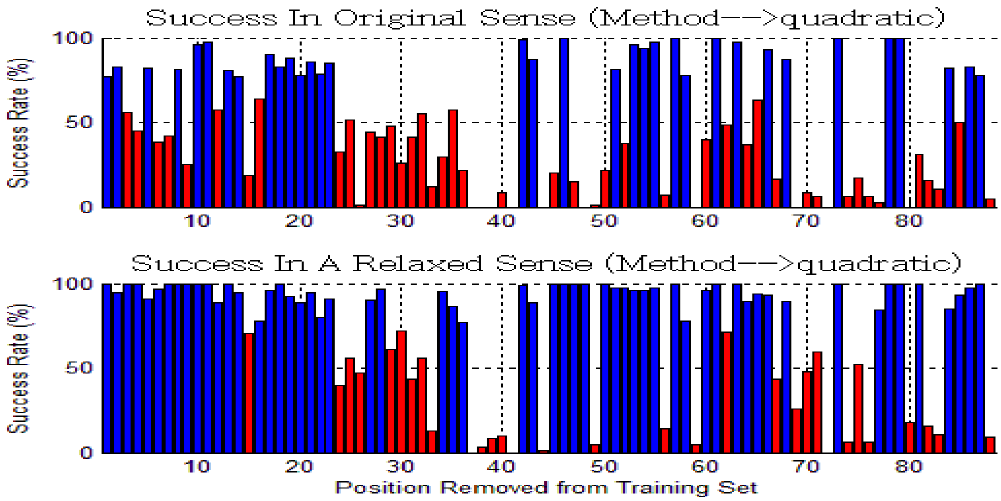


Figure 24: Success rate in classifying data obtained from different test locations (*quadratic*).

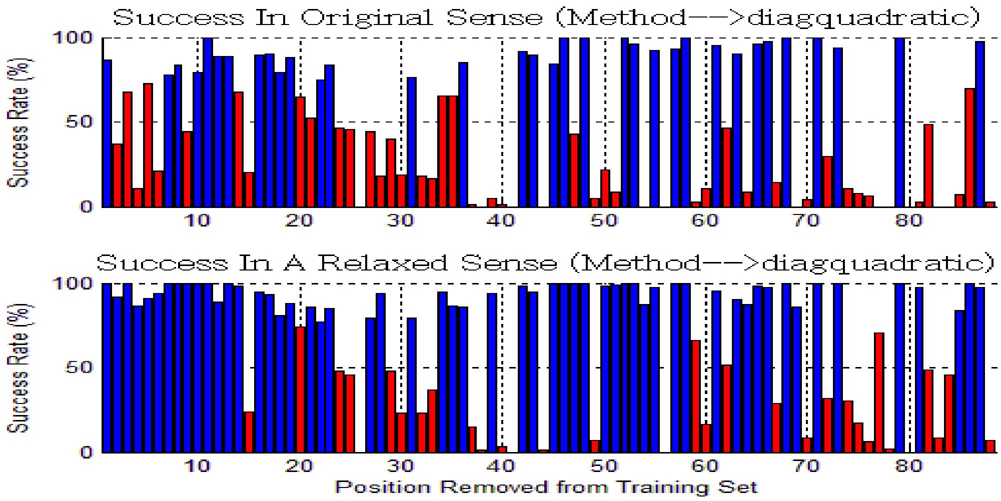


Figure 25: Success rate in classifying data obtained from different test locations (*diagquadratic*).

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

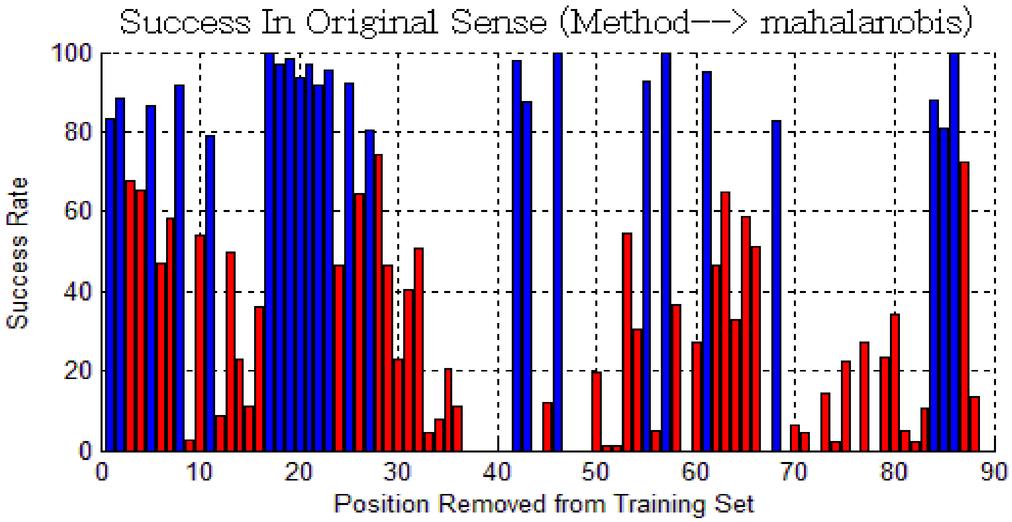


Figure 26: Success rate in classifying data obtained from different test locations (*mahalanobis*).

Figure 27 to Figure 31 show the distribution of the room numbers, obtained by solving the classification problem. What is shown is the probability that a particular room was the source of the signal. For instance, in the figure for room 1, the algorithm indicates that the probability that the signal originates from Room 1 is slightly above 50%, and that the probability it originates from Room 3 is slightly less than 50%, and that there is a very small probability it originates from Room 6. Therefore, we can say with high confidence the signal originates from Room 2 or its direct neighbors. From these figures one can easily observe that we are able to track the signal source up to an accuracy of its neighborhood, almost all the time (>90%). This is a very encouraging result.

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

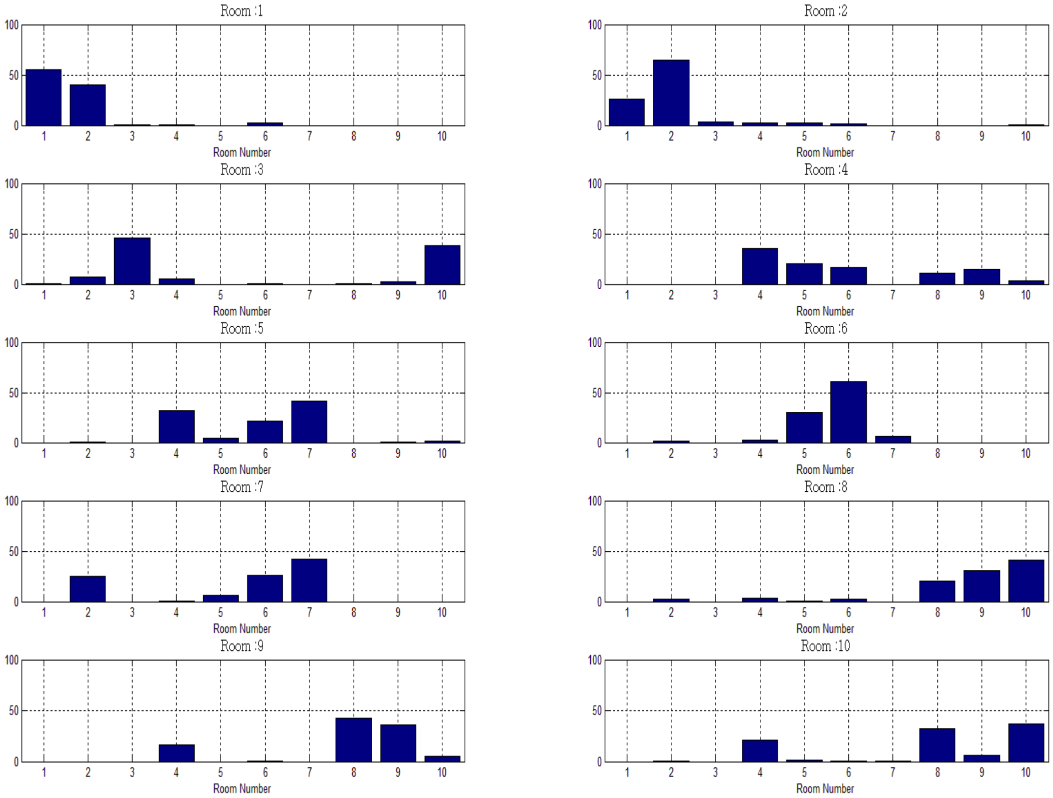


Figure 27: Distribution of the most probable room (*linear*).

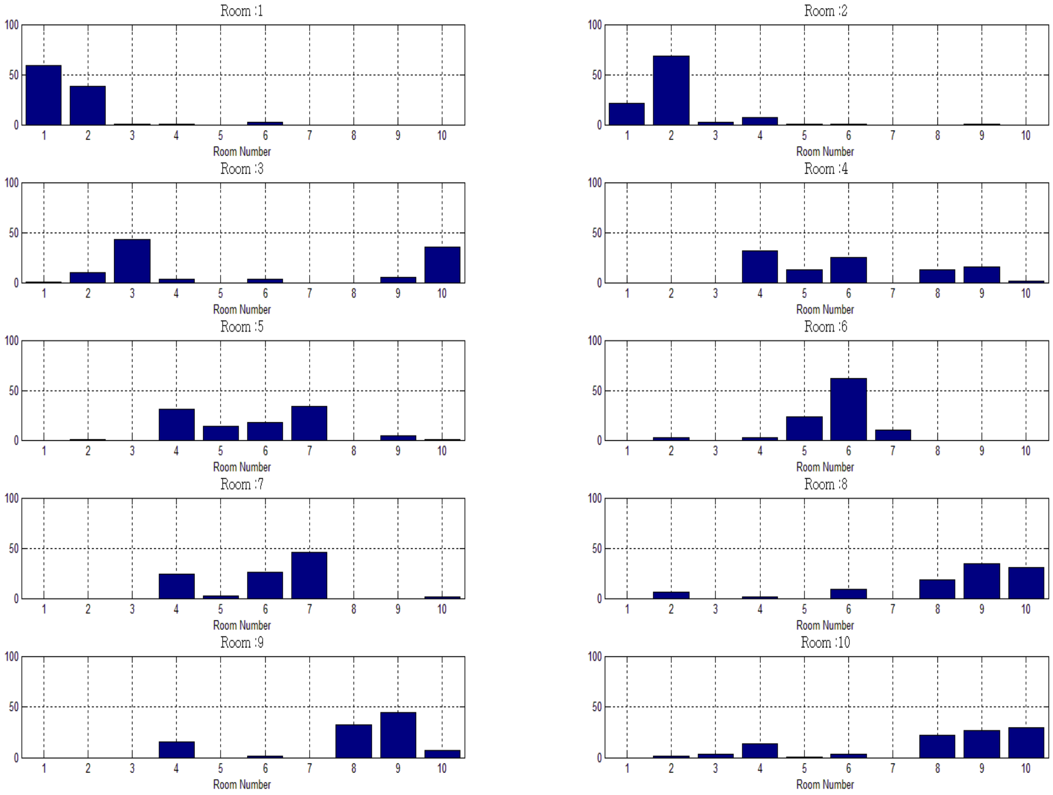


Figure 28: Distribution of the most probable room (*diaglinear*).

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

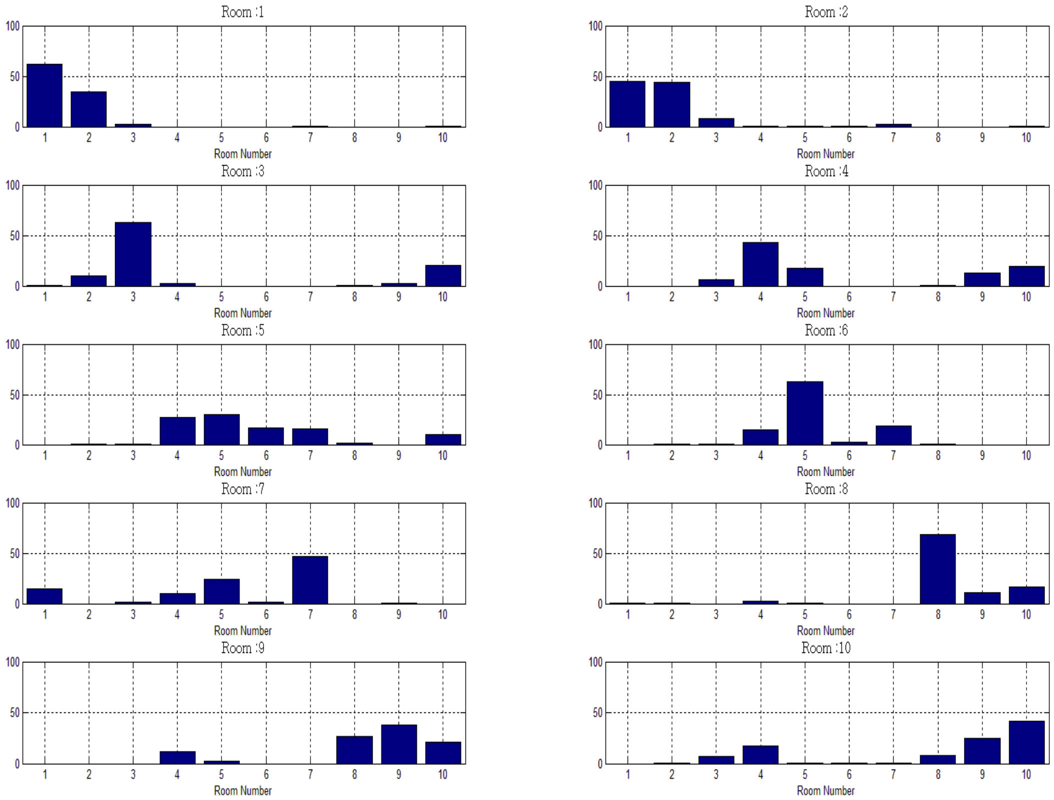


Figure 29: Distribution of the most probable room (*quadratic*).

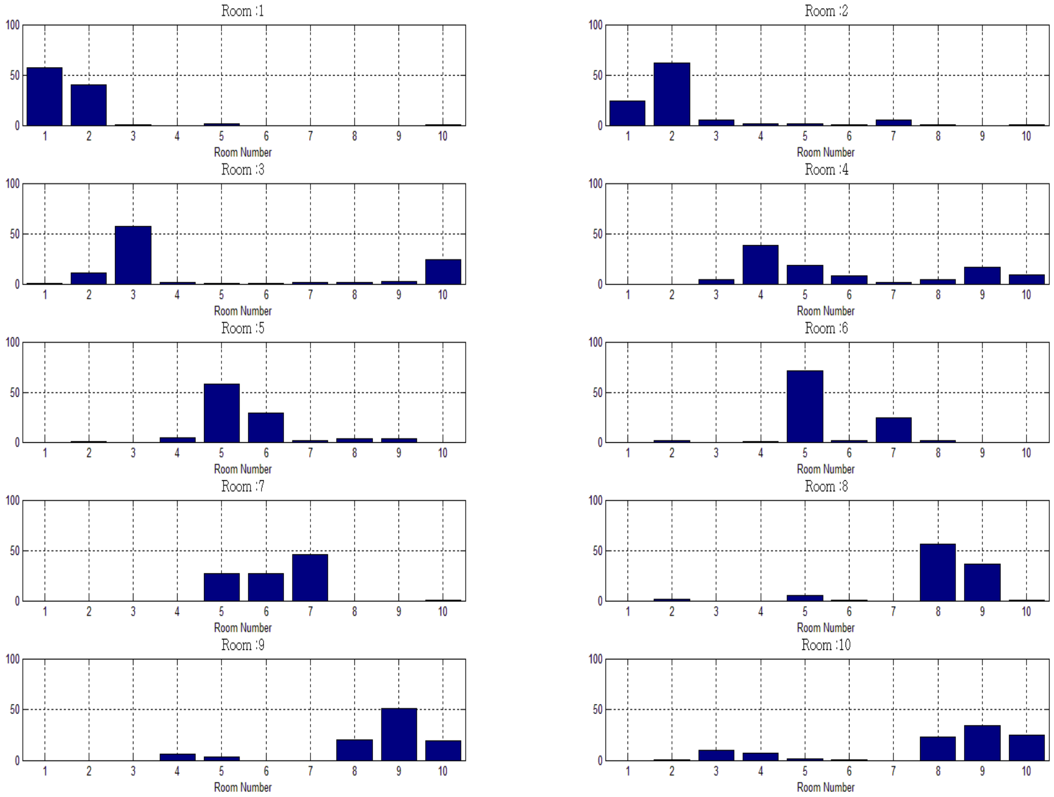


Figure 30: Distribution of the most probable room (*diagquadratic*).

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

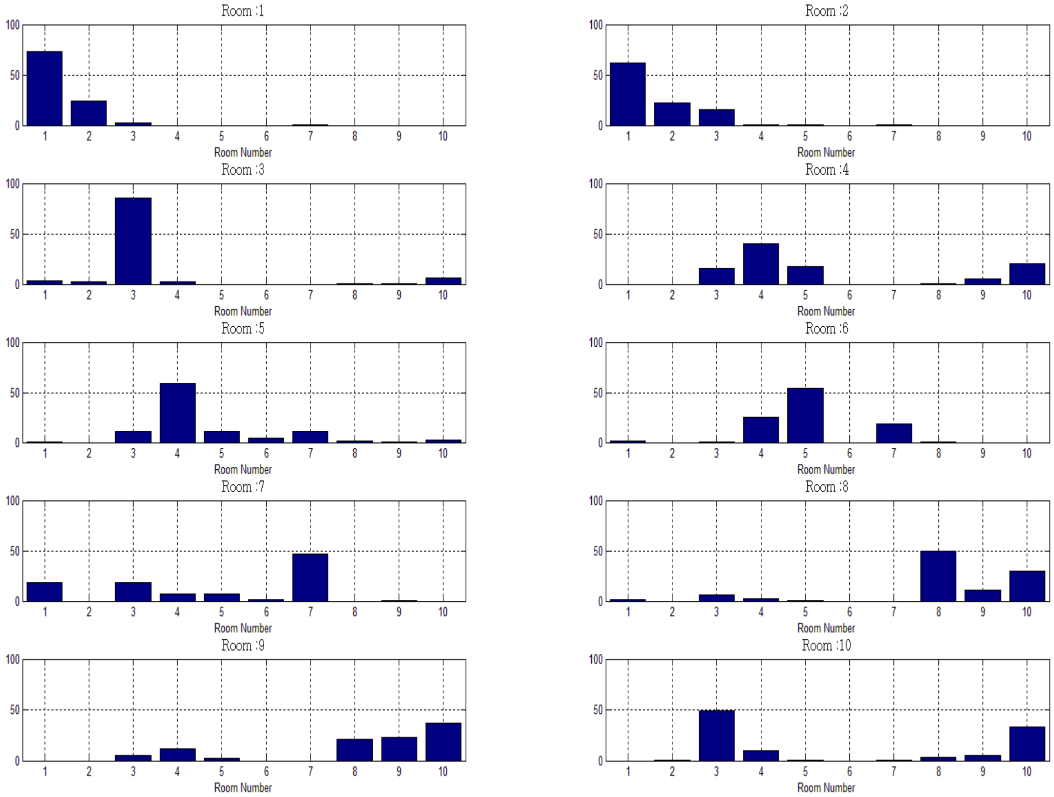


Figure 31: Distribution of the most probable room (*mahalanobis*).

4.8 Histogram Features

As we have discussed, the *classify* routine of MATLAB makes two assumptions which are very crucial for a satisfactory performance of the classifier.

- Firstly it assumes the features, from a particular class, have a multivariate Gaussian distribution.
- Secondly it assumes uniform prior distribution, unless otherwise stated.

While the second assumption seems to be reasonable, the validity of the first assumption should be put under a through scrutiny.

The histograms of different features from all of the ten rooms, as shown in Figure 32 to Figure 38, indicate that the assumption on normality doesn't hold true for the problem of interest. This claim can also be verified intuitively. The way the signal strength is defined, it can never take a negative value, but according to the normality assumption the probability of getting a negative value for signal strength can never be zero. Thus it can be concluded that the inbuilt classify routine might not be best candidate to serve our requirements. Alternatively, we can apply the *k*-nearest neighbor (*k*-NN) approach to solve the classification problem. Adaptation of *k*-NN approach will result in increased degrees of freedom for the classification problem, as the neighborhood size (*k*) and the definition of distance need to be selected before solving the problem.

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

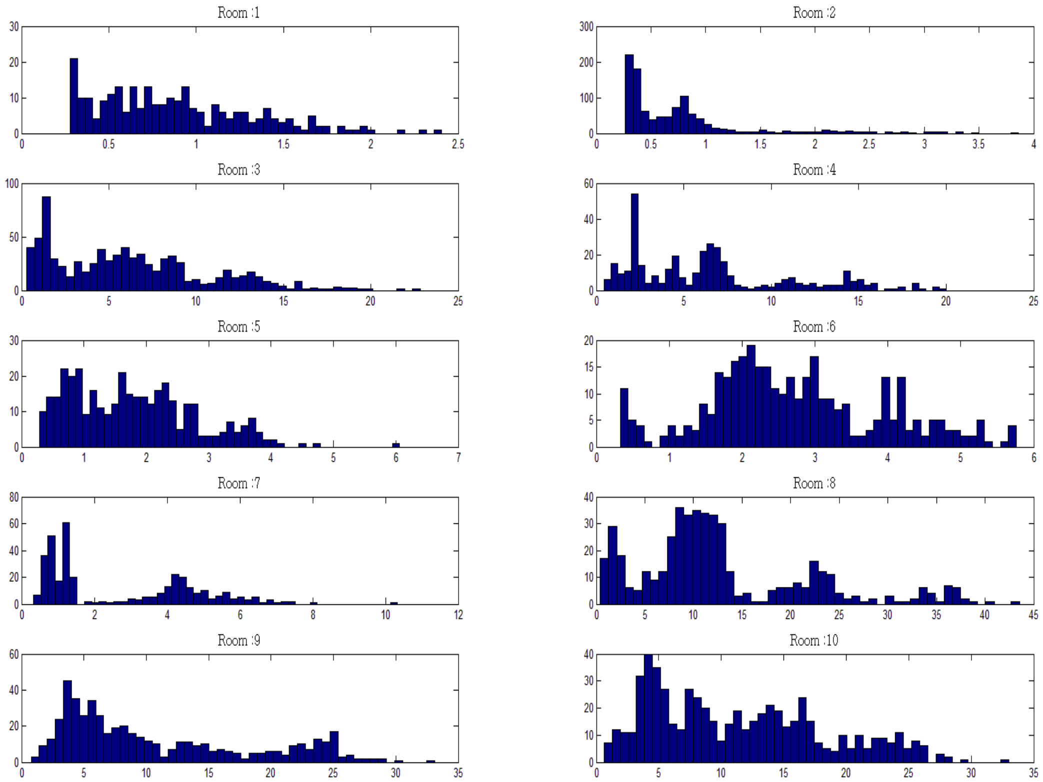


Figure 32: Distribution of the strength of the signal received at antenna 1, in different rooms.

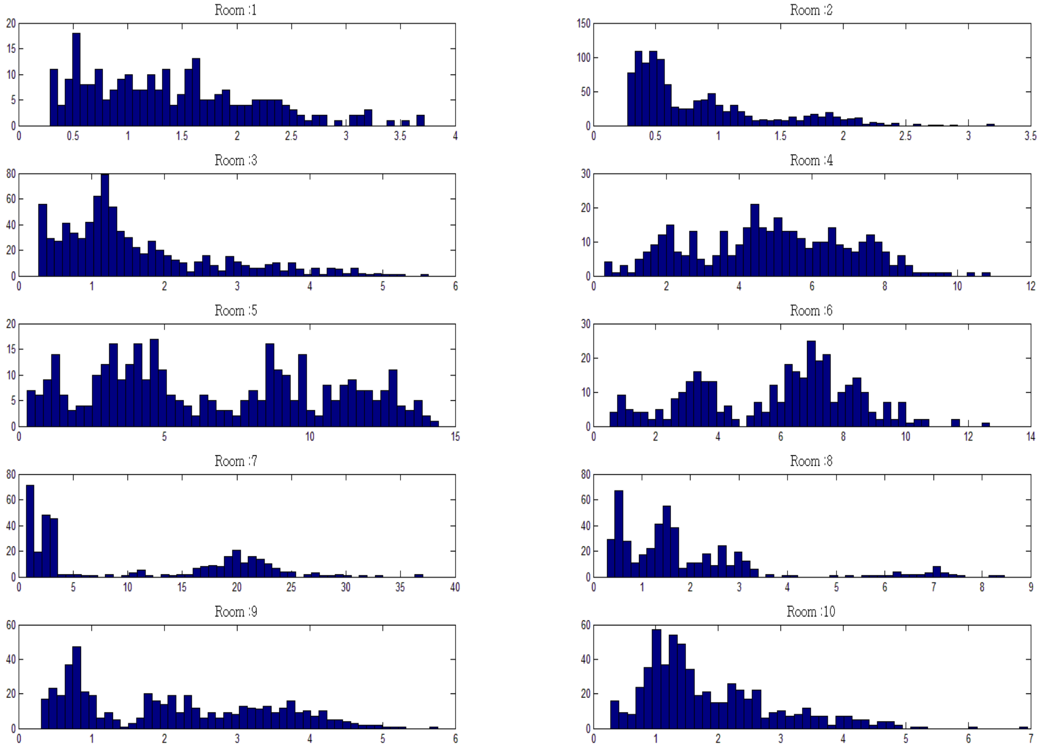


Figure 33: Distribution of the strength of the signal received at antenna 2, in different rooms.

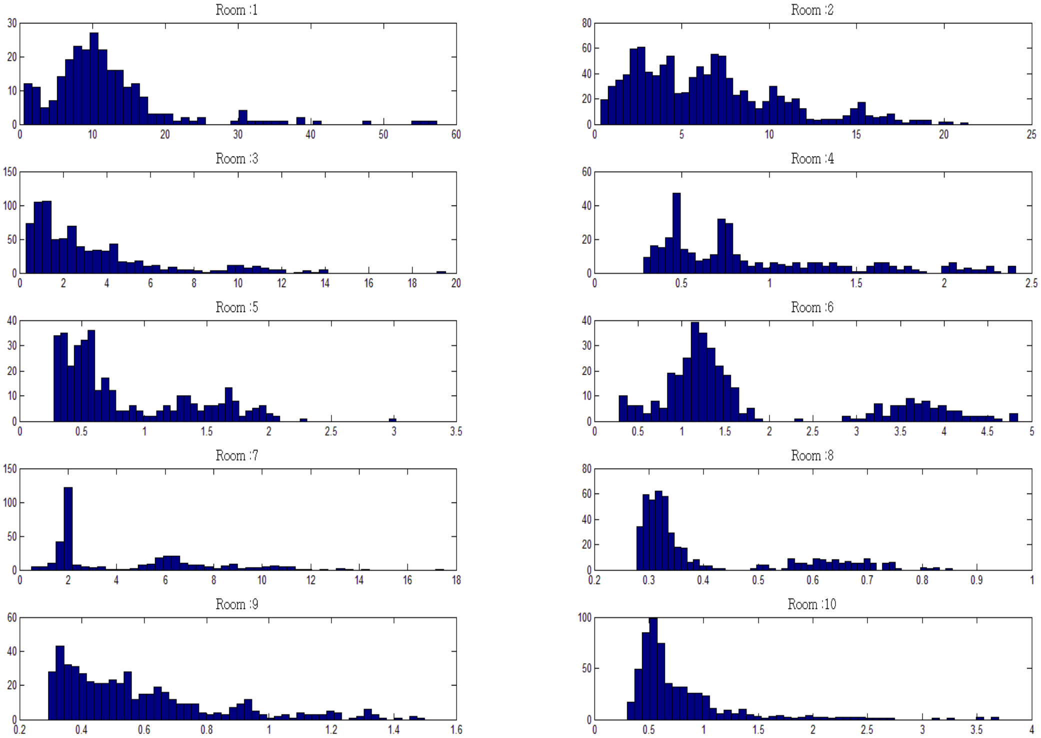


Figure 34: Distribution of the strength of the signal received at antenna 3, in different rooms.

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

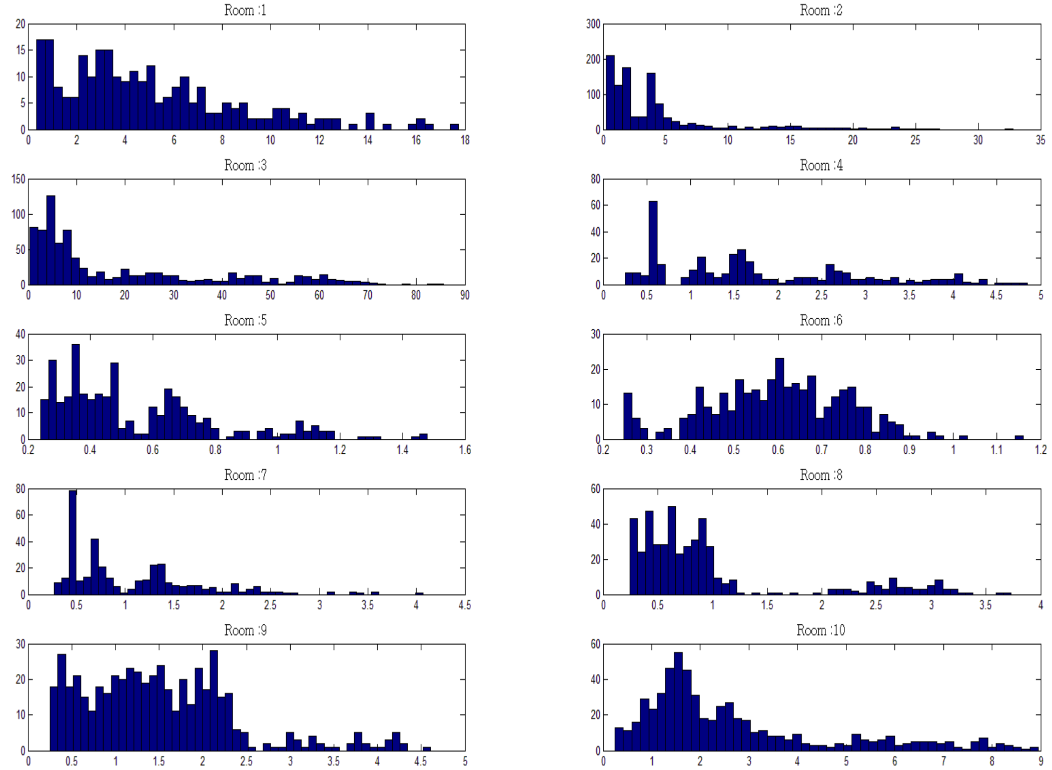


Figure 35: Distribution of the strength of the signal received at antenna 4, in different rooms.

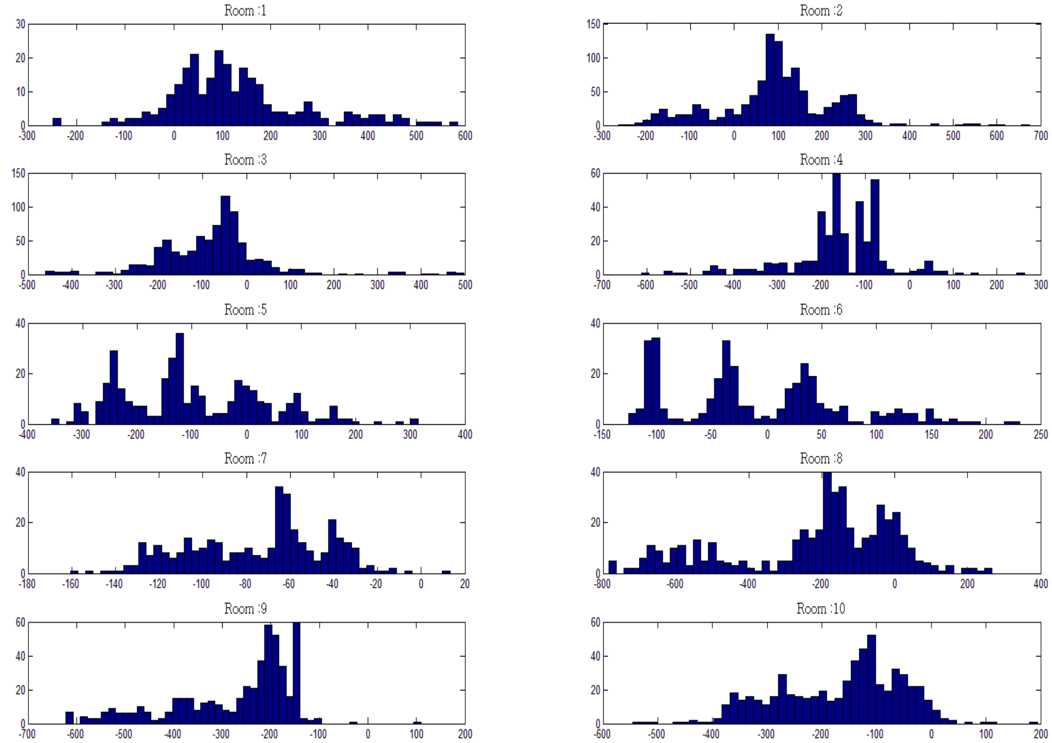


Figure 36: Distribution of the TDOA between the signal received at antenna 1 and the signal received at antenna 3, in different rooms.

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

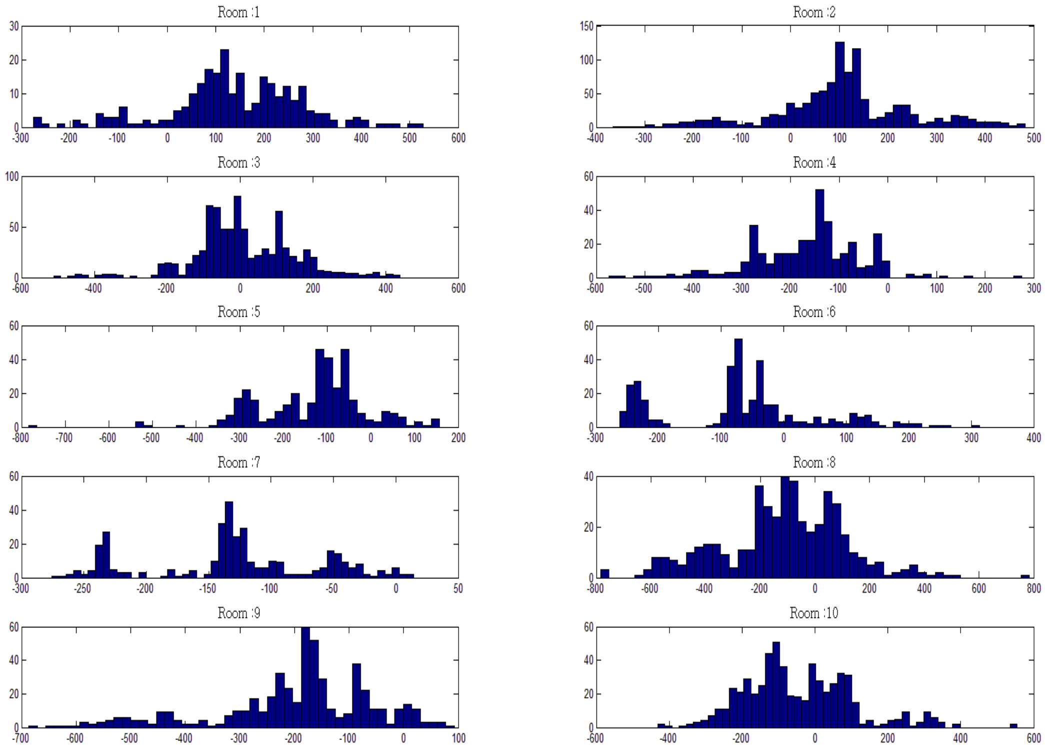


Figure 37: Distribution of the TDOA between the signal received at antenna 2 and the signal received at antenna 3, in different rooms.

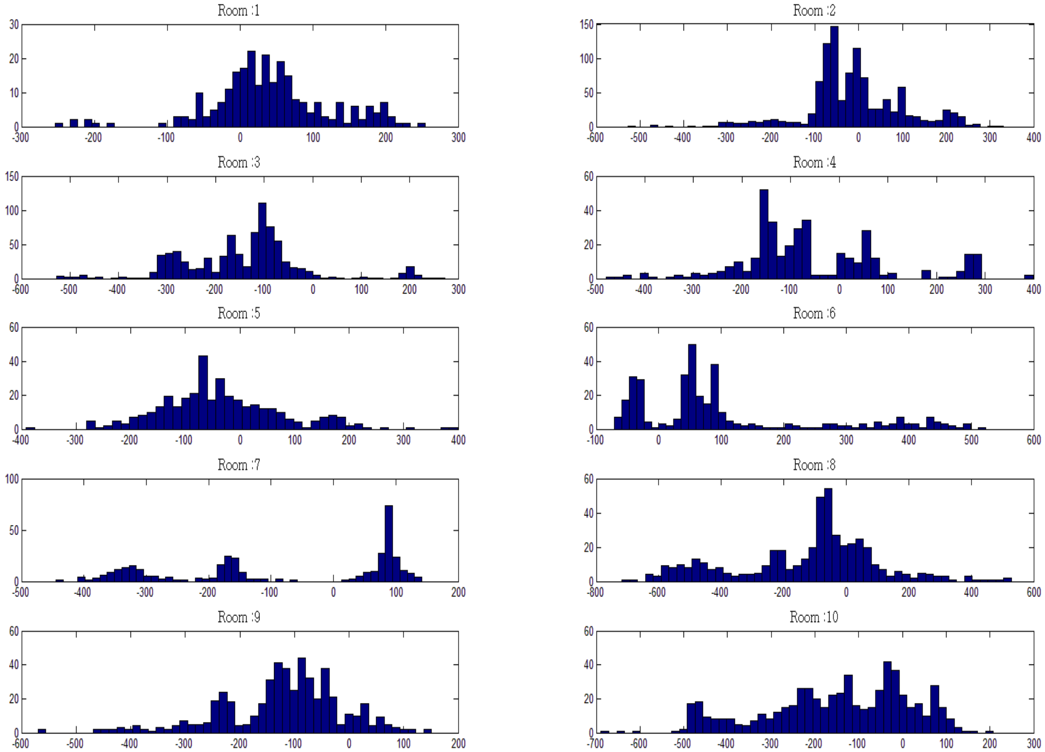


Figure 38: Distribution of the TDOA between the signal received at antenna 4 and the signal received at antenna 3, in different rooms.

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

5. Experiments and Results

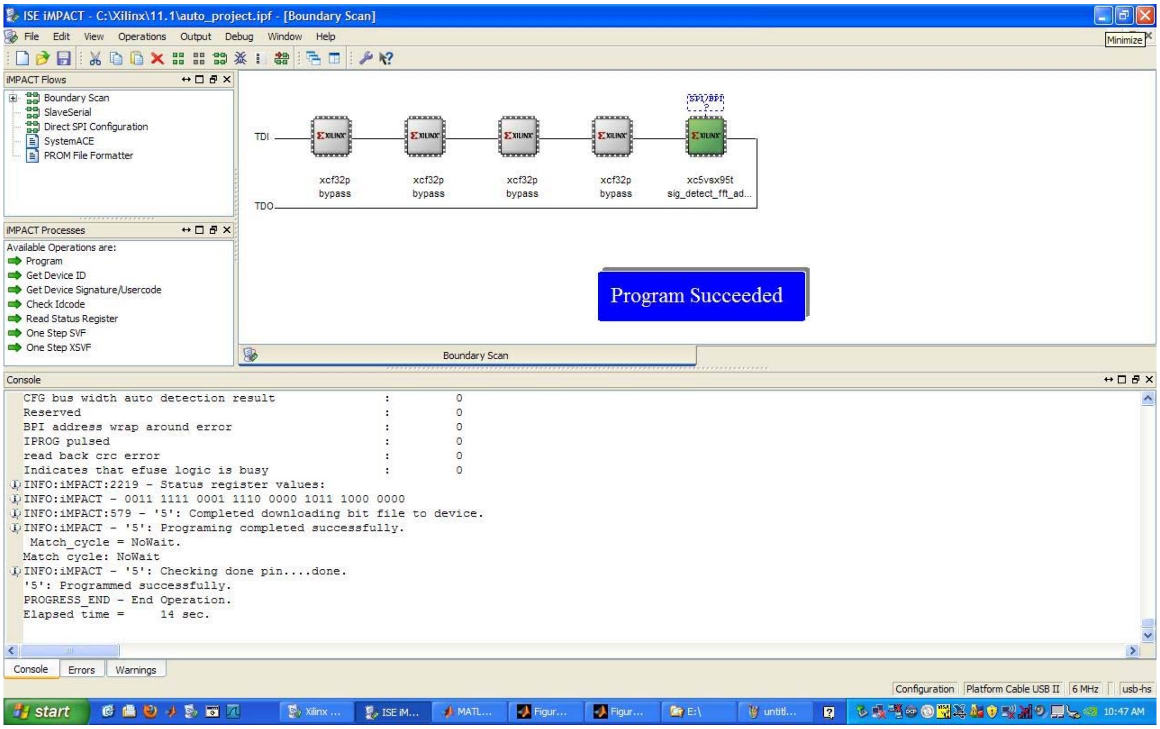
We did extensive field testing in IAI office building. The office environment is similar to a prison environment in that: there is no line of sight and between the transmitter and receiving antennas, and the environment is not static (i.e., door open and close and furniture and items move around periodically). It is different from a prison in that for a prison: the doors are metal instead of wood, the walls are concrete instead of drywall/wood, and that prisons have larger open spaces (hallways). In spite of the differences, the office presents a convenient place to collect large amount of data and we feel it is similar enough to make initial conclusions.

5.1 Steps for System Operating and Testing

5.1.1 Data Acquisition

Input to MATLAB program is provided via 4 receiving FPGA boards through sig_detect_fft_adc_single.bit program accessible by Xilinx programming tool and GUI, ISE iMPACT (Figure 39).

- Sets transmitter and receiver parameters
- Performs simple I/O
- Performs analysis on simulated data if desired
- Sets variables to accommodate FGPA messages
- Communicates with FPGA via socket programming in Matlab
- Saves and plots the received raw data



```
  CFG bus width auto detection result              :        0
  Reserved                                         :        0
  BPI address wrap around error                    :        0
  IPROG pulsed                                     :        0
  read back crc error                              :        0
  Indicates that efuse logic is busy               :        0
INFO:iMPACT:2219 - Status register values:
INFO:iMPACT - 0011 1111 0001 1110 0000 1011 1000 0000
INFO:iMPACT:579 - '5': Completed downloading bit file to device.
INFO:iMPACT - '5': Programing completed successfully.
   Match_cycle = NoWait.
  Match cycle: NoWait
INFO:iMPACT - '5': Checking done pin....done.
  '5': Programmed successfully.
  PROGRESS_END - End Operation.
  Elapsed time =      14 sec.
```

Figure 39: FPGA data acquisition interface

5.1.2 Feature Extraction

Features to consider: a) the signal strengths at four different signals and b) the time difference of arrival (TDOA) at antenna number 1, 2 and 4 with respect to the antenna at location 3.

- Signal strength is calculated as the absolute mean of the received voltages.
- To get the TDOA between two received signals we have to find out the correlation peak between them.
  - First, the received signals go through a 100th order band-pass filter to isolate the channels of interest
  - The channel frequency is removed without knowing its exact value by low pass filtering the square of the correlated signal. The correlation is squared in order to present a DC component to the low pass filter. A sharp 400th 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 correlation curve is smoothed 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.
  - The peak index of each filtered and smoothly correlation is found and these indexes are converted to delays in nanoseconds using a linear function.

5.1.3 Outlier Removal

Outlier removal is done in 2 stages:

- Throw away any observation if any of the four receiving antennas gets the transmission outside the frequency band of our interest. The channels the modem uses to use is not under our control, it is directed to the modem by the cellular tower.
- Compute the mean (μ_l^i) and standard deviation $(\sigma_l^i)$of a particular feature "i" obtained from a particular location"l". Throw away all the observations where either of the seven feature values lies outside the $(\mu_l^i \pm 3\sigma_l^i)$ region.

5.1.4 Data Classification

Data classification is done based on 3 mehtods:

- Matlab inbuilt classifier
- Support Vector Machine (SVM) classifier
- Laplacian-based classifier

5.2 Test Plan and Map

A considerable amount of landmarked data was required to train our classification algorithm. One portion of the IAI office complex (Figure 40) was used as a model environment for testing purpose. A cellular modem (MultiTech MTCBA-C1), using the CDMA2000 cellular protocol over the Verizon network, was used as the transmitter, as well as several cell phones from Verizon, AT&T and T-Mobile. The receiving system consists of one FPGA processor with four high-speed front-end receiver boards, each connected with one antenna port. Long cables, each >300ft, extend from each receive ports to antennas located at each corners of the office. Since the same hardware is used to sample all four channels, synchronization is not an issue after calibrating for small

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

differences in cable length. The same hardware is used to sample all four channels. Figure 41 shows the overall system design.

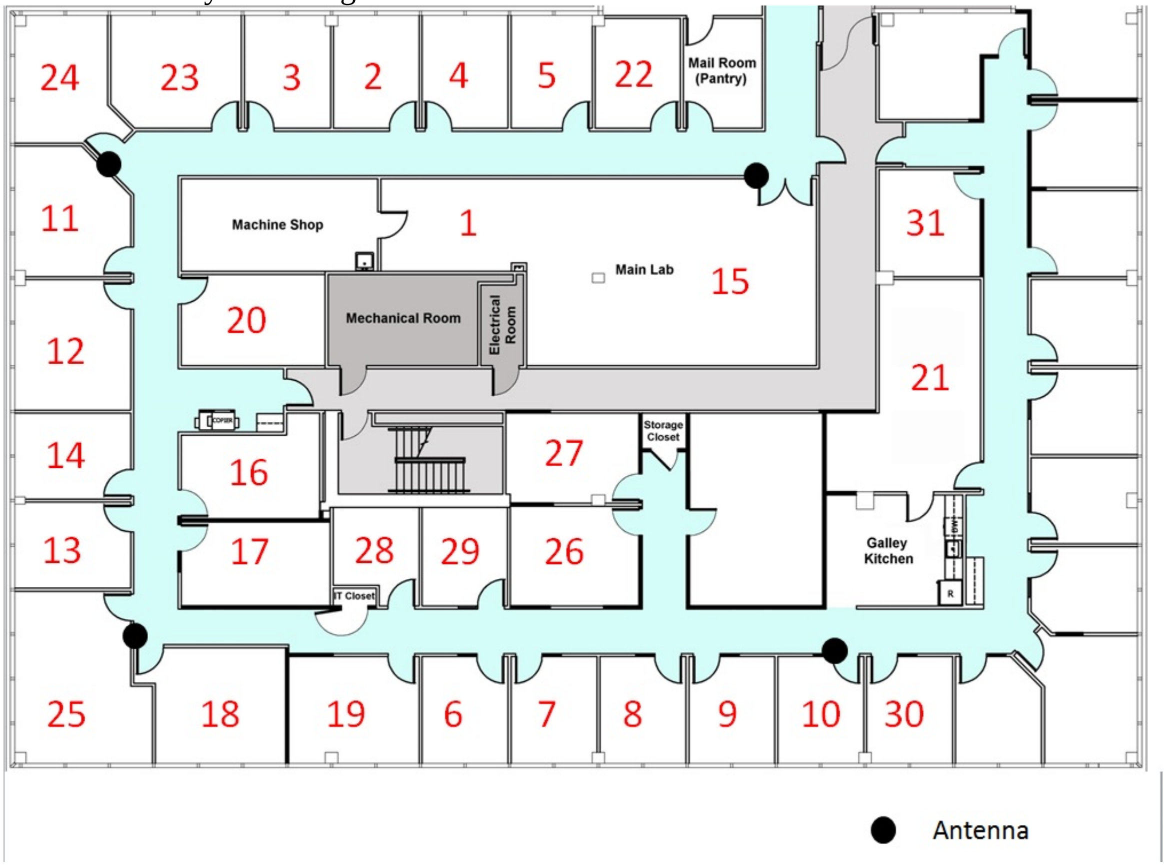


Figure 40: Cell phone test map

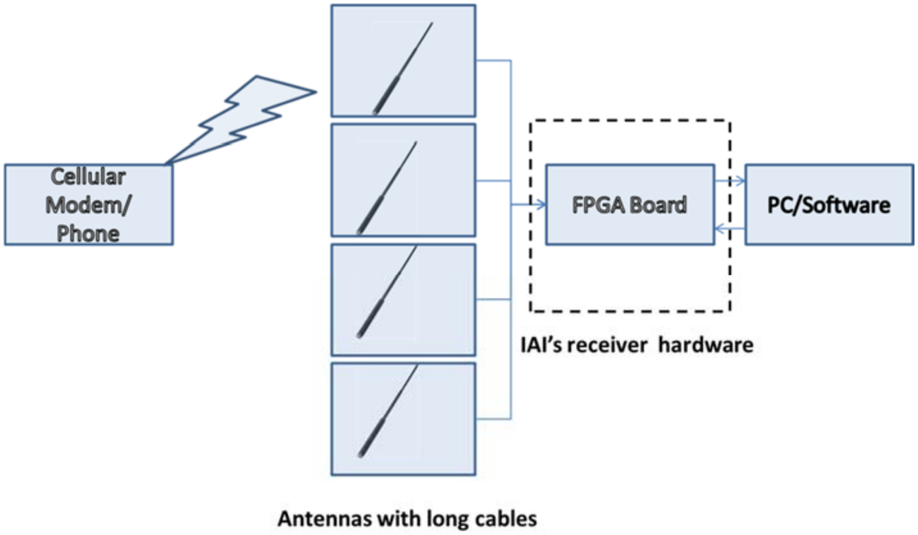
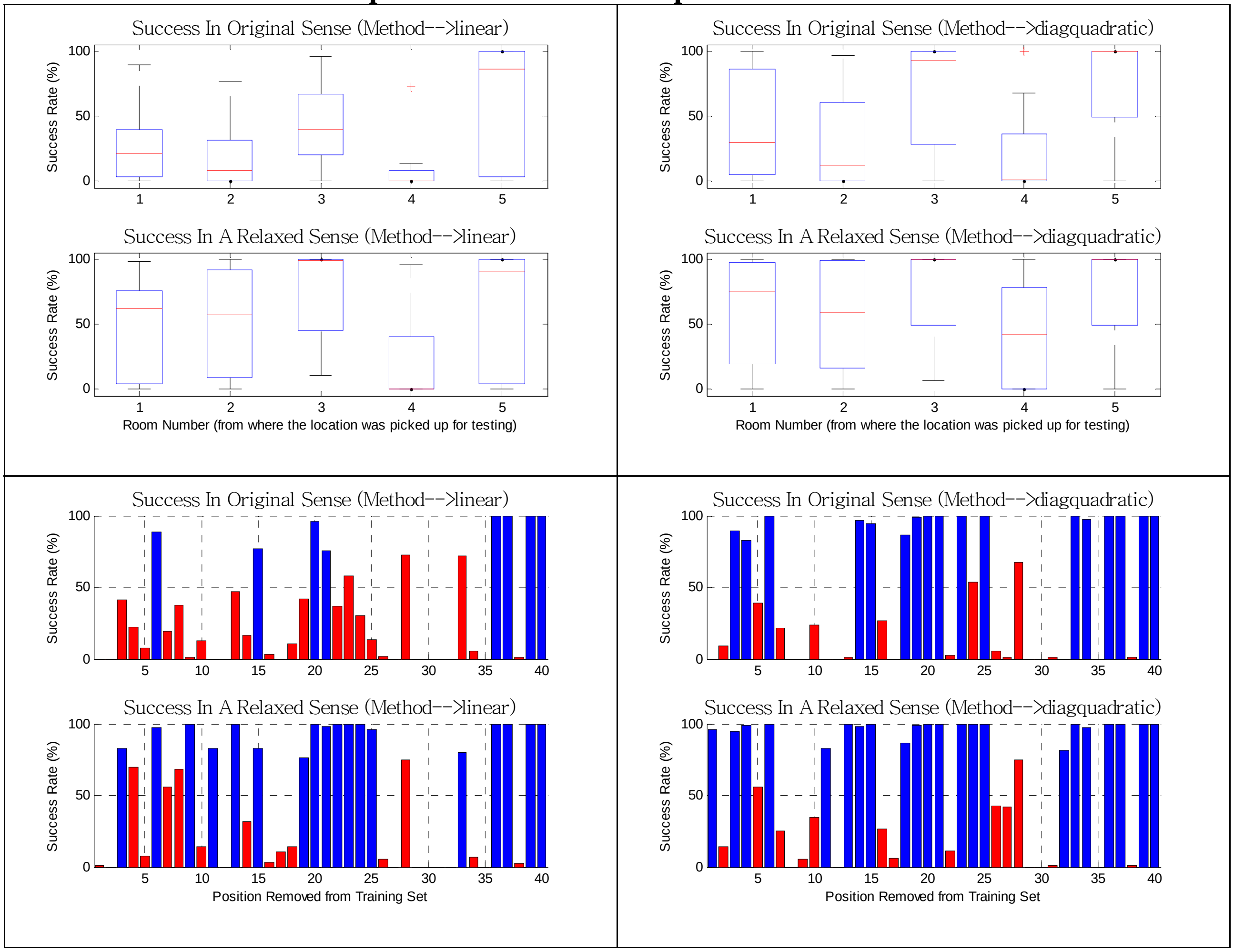


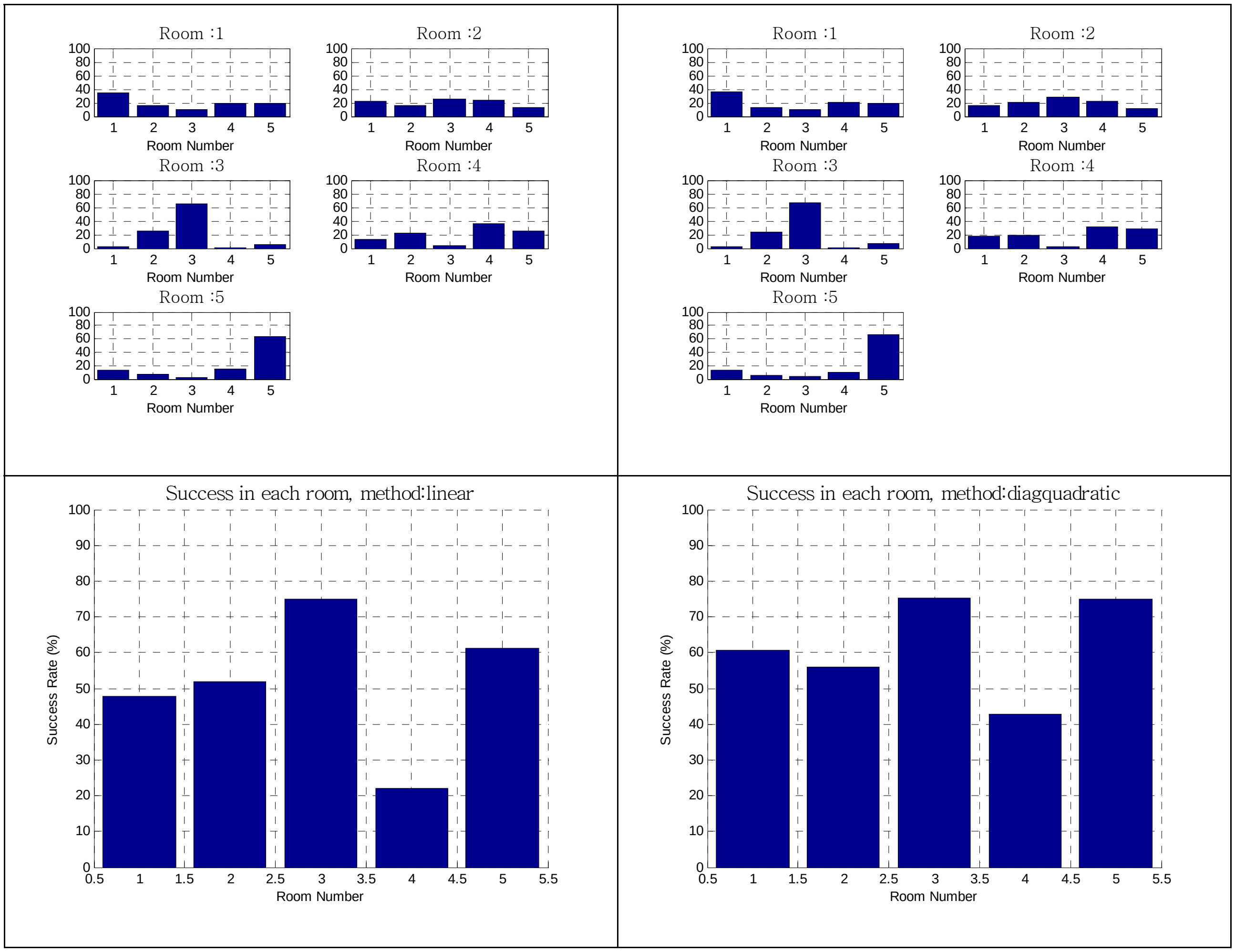
Figure 41: Overall system design

We conducted cell phone transmission experiments in IAI building. Figure 40 shows the test map for our cell phone experiments. In this map, four antennas are placed at the four corners of the building. Each room is assigned a room ID for testing and verifying purposes, as shown in Figure 40. Due to the limited time in collecting data, we have not covered all the rooms in this map at this time. In the experiments, a Verizon CDMA modem with a cell phone number, which registered and activated in Verizon wireless network, is used to transmit the data.

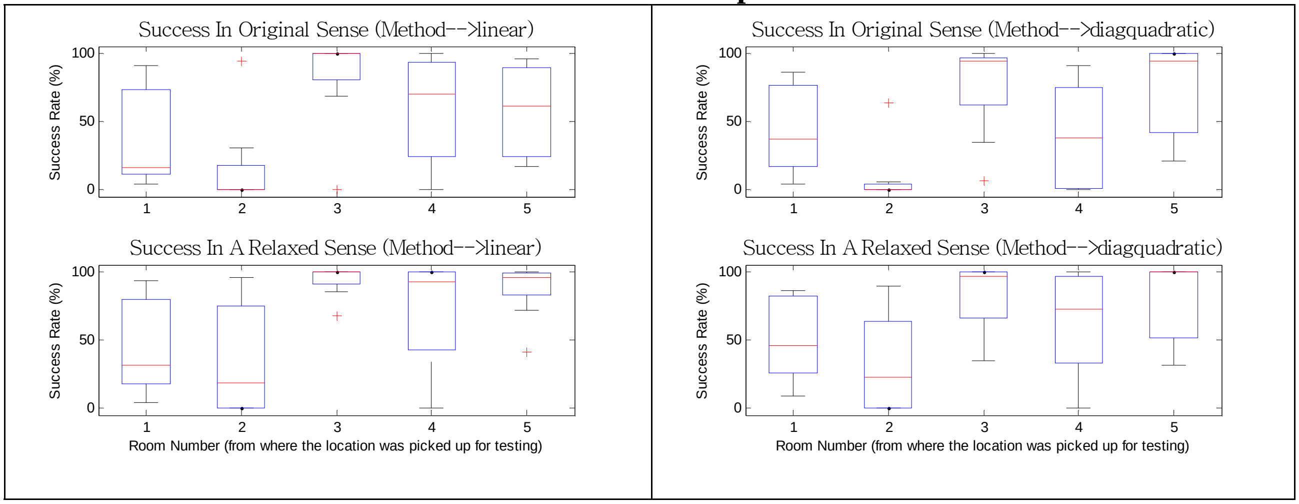
5.3 Scenario 1: Door-open 50-transmission Experiments



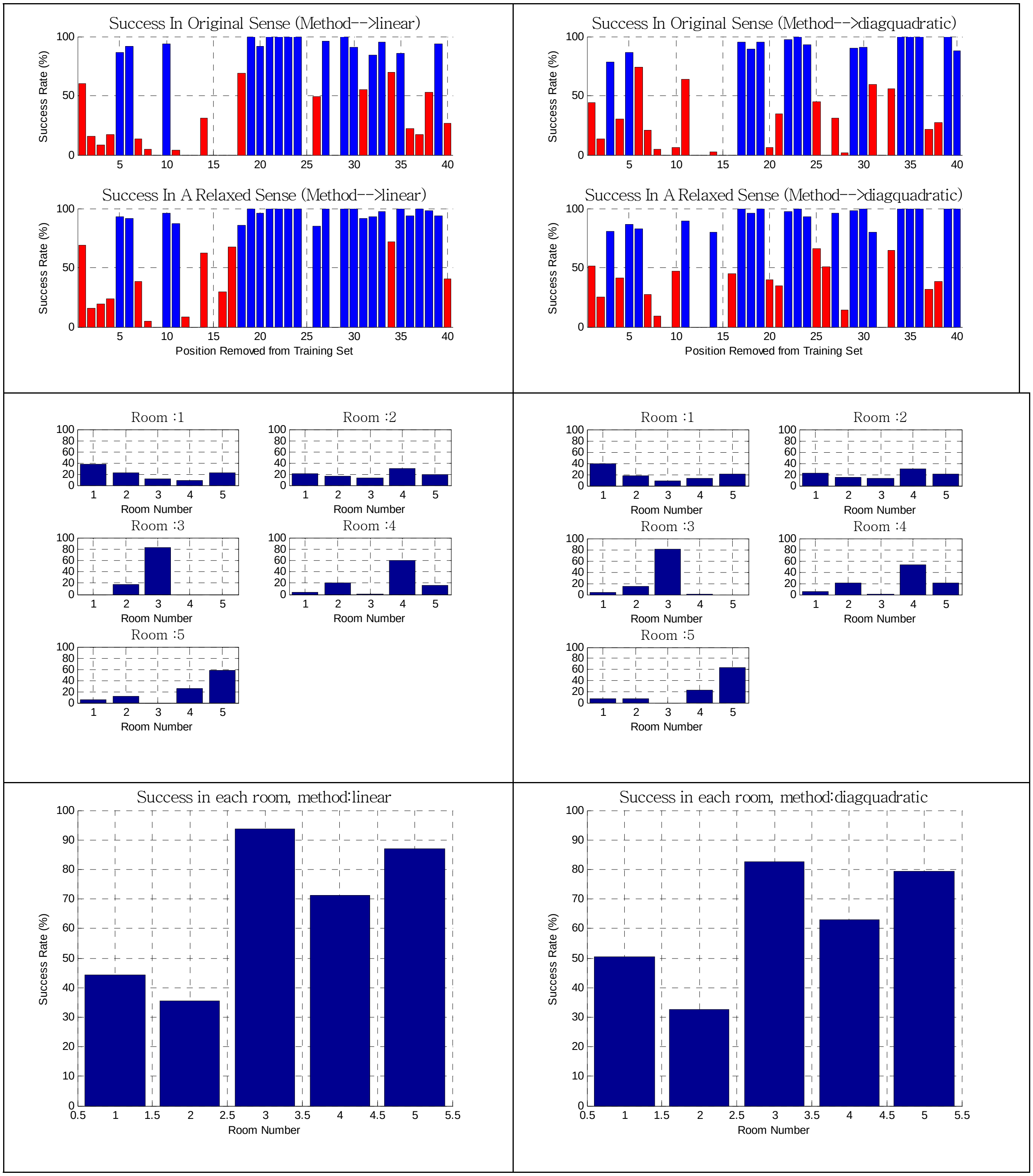
This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.



5.4 Scenario 2: Door-closed 50-transmission Experiments



This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

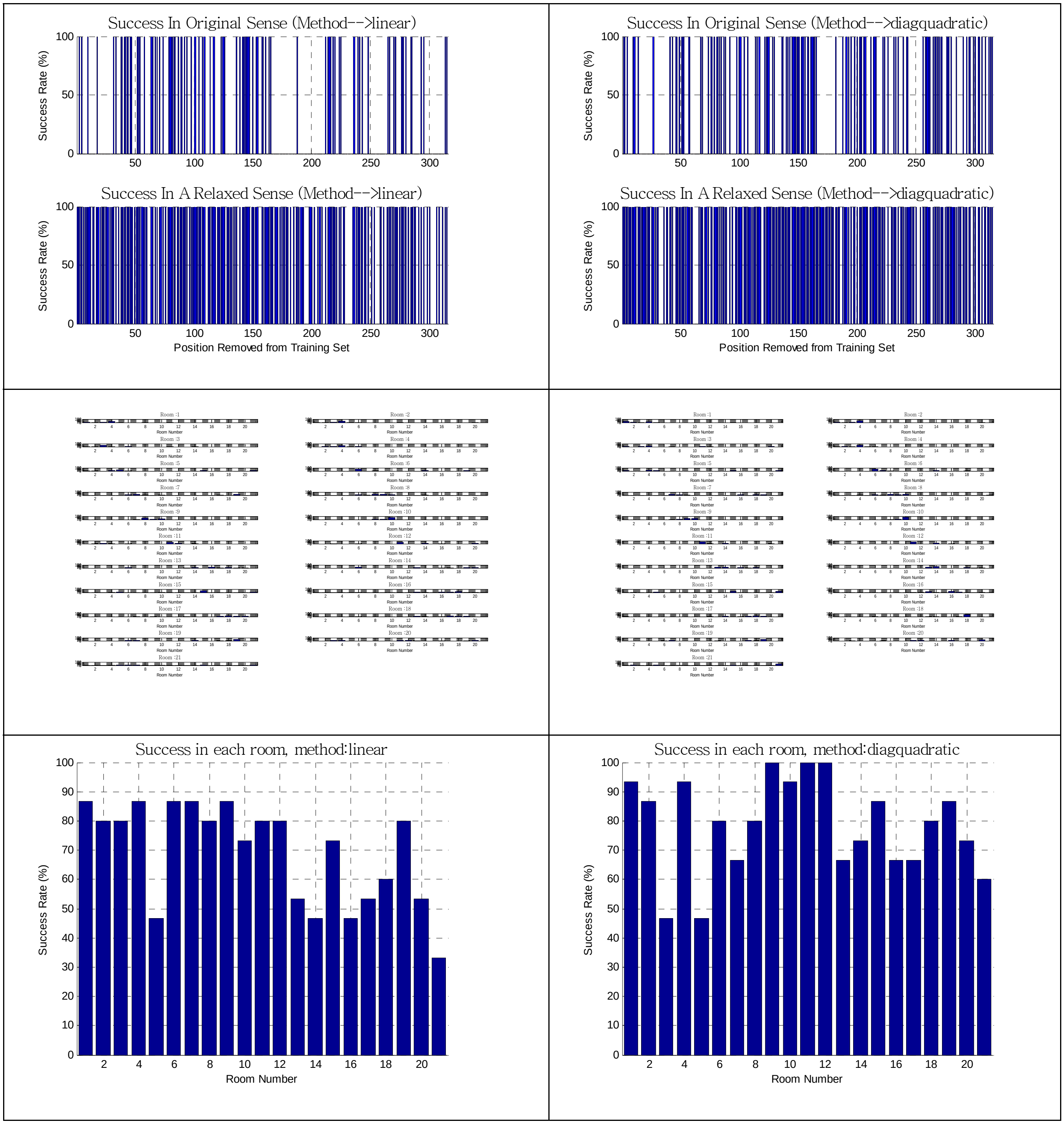


5.5 Scenario 3: Cell phone On-Off Experiments

When each time a cell phone is turned on, it communicates with base station within a short time period. In the prison scenario, it is highly possible that we are able to capture this signal right after a person just turns on a cell phone. Thus, the following experiments are conducted.

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

In this On-Off test, we selected 15 different positions in each room, which covers most area of each office. At each position, the modem was powered on from previous off status. Then, in the following 30-60 seconds, we are able to receive 1-3 signals that are sent by our modem. Based on this small amount of data, we run the classification algorithm.

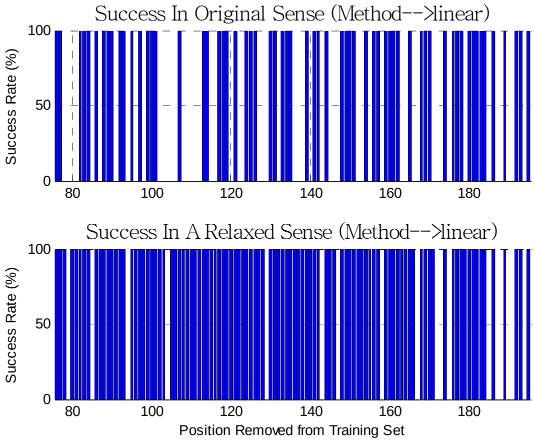


This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

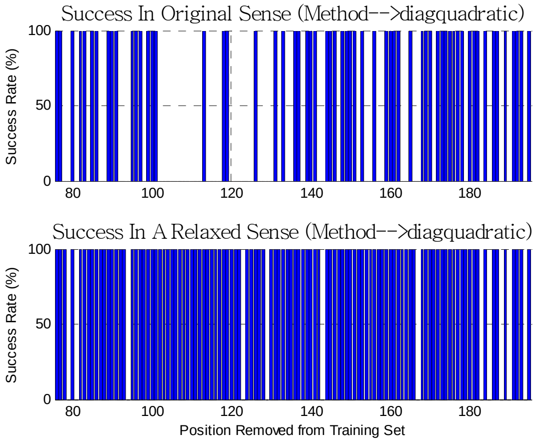
Both linear method and dia-quadratic method are adopted. Dia-quadratic method shows better performance than linear method.

5.6 Scenario 4: Door-closed 10-transmission Experiments

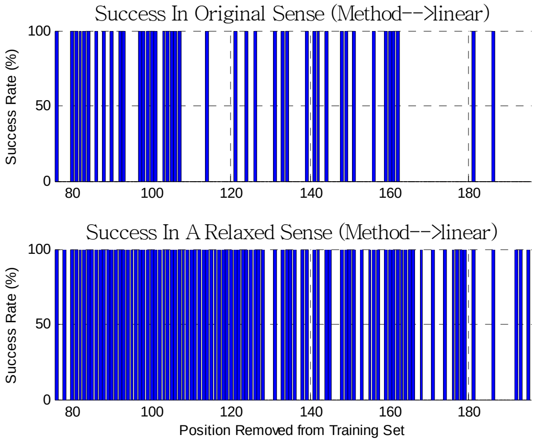
These sets experiments are similar with Scenario 2, but have more positions and fewer transmissions in each room. 15 different positions are selected and 10 cell phone transmission signals are captured. Due to the time limitation, data sets are not collected in all rooms.



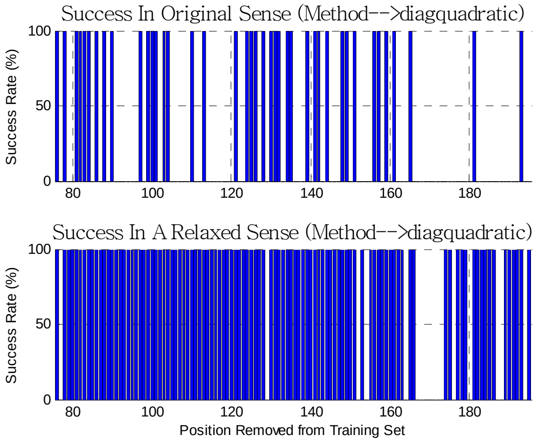
Average of 7 features, 10-transmission data to train, 10-transmission data to test, linear



Average of 7 features, 10-transmission data to train, 10-transmission data to test, diagquadratic

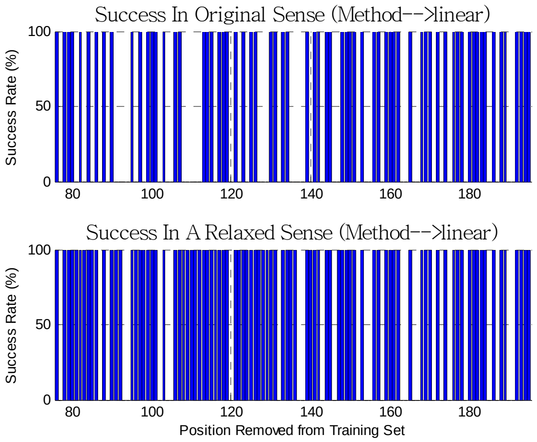


Average of 7 features, On-Off data to train, 10-transmission data to test, linear

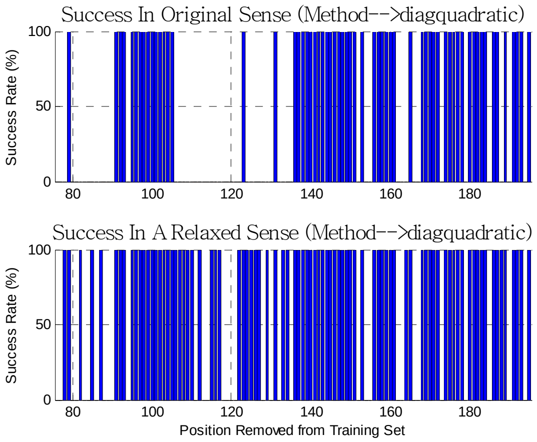


Average of 7 features, On-Off data to train, 10-transmission data to test, diagquadratic

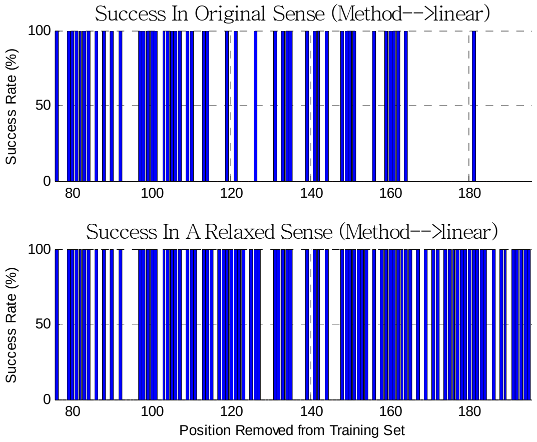
This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.



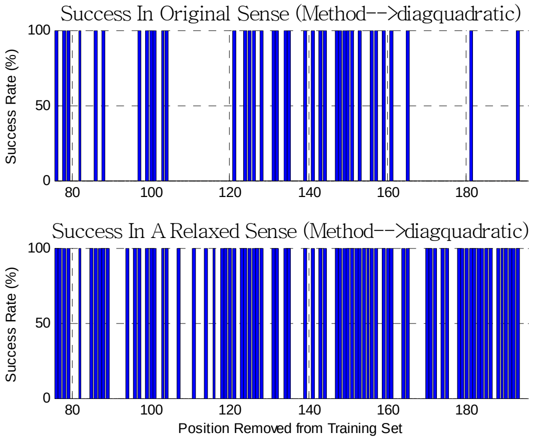
Average of 10 percentages, 10-transmission data to train, 10-transmission data to test, linear



Average of 10 percentages, 10 transmission data to train, 10-transmission data to test, diagquadratic

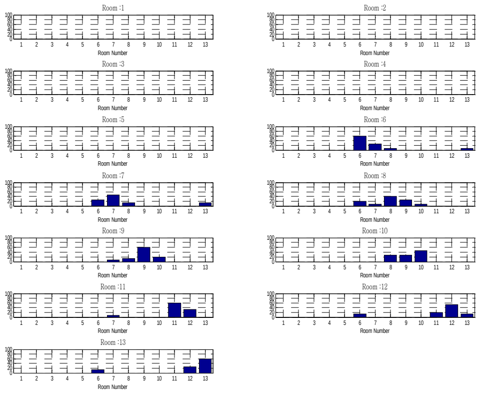


Average of 10 percentages, On-Off data to train, 10-transmission data to test, linear

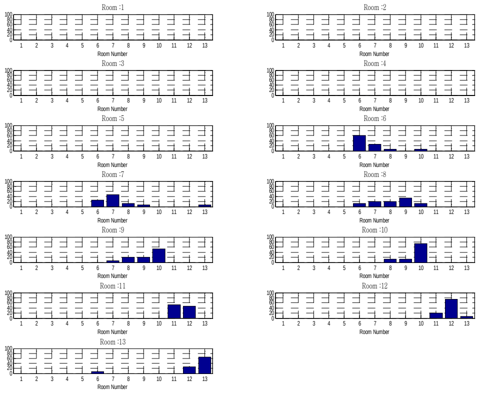


Average of 10 percentages, On-Off data to train, 10-transmission data to test, diagquadratic

Classification results of each room are shown here:

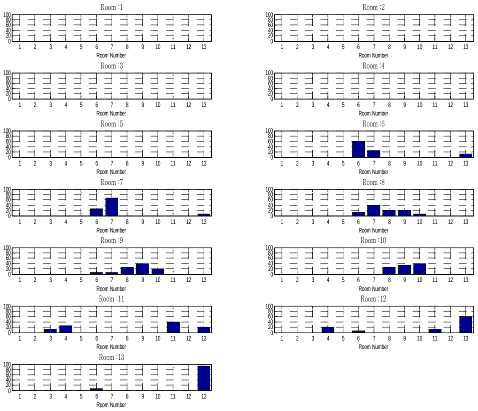
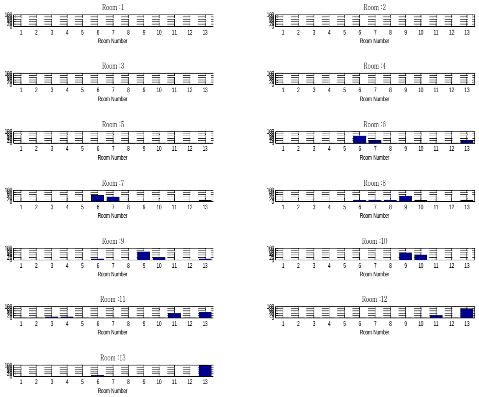
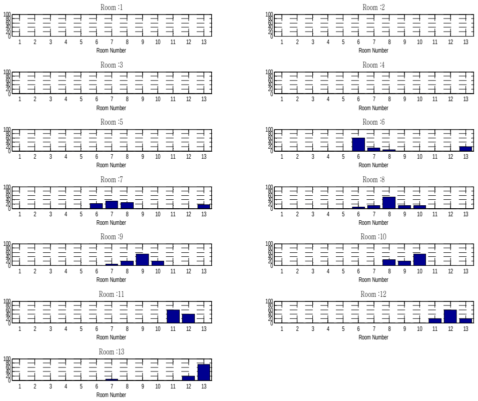
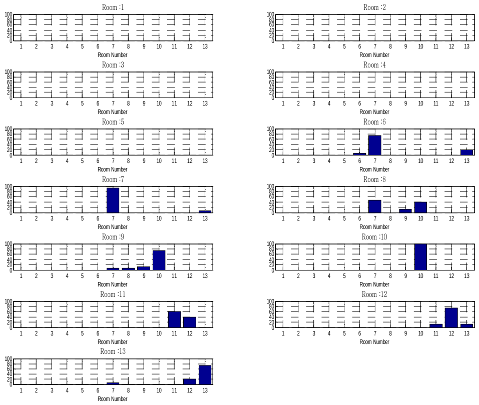
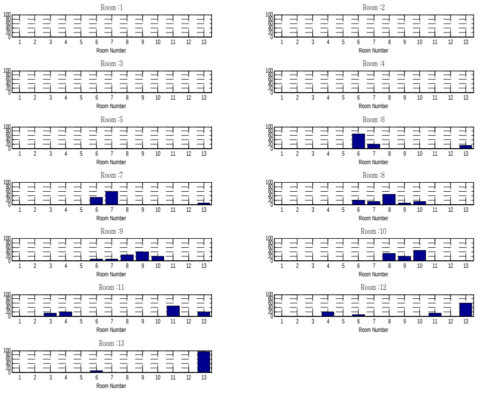
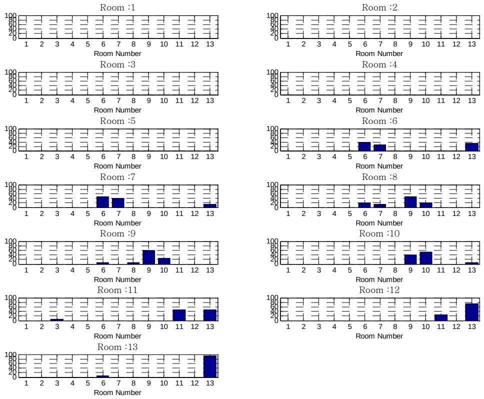


Average of 7 features, 10-transmission data to train, 10-transmission data to test, linear



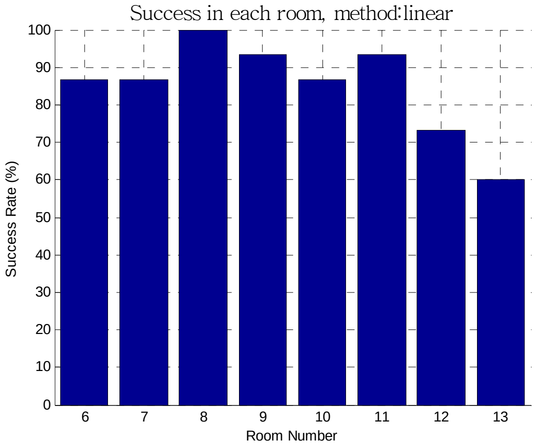
Average of 7 features, 10-transmission data to train, 10-transmission data to test, diagquadratic

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

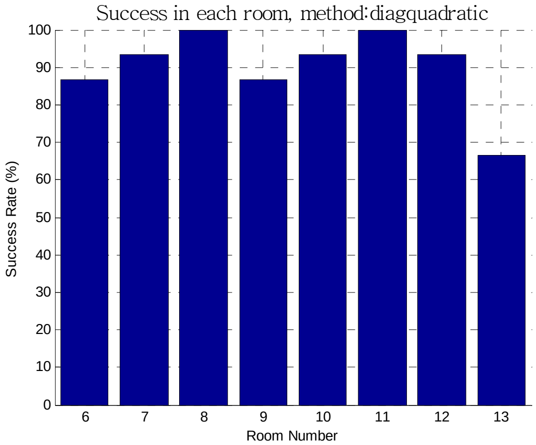
 Average of 7 features, On-Off data to train, 10-transmission data to test, linear	 Average of 7 features, On-Off data to train, 10-transmission data to test, diagquadratic
 Average of 10 percentages, 10-transmission data to train, 10-transmission data to test, linear	 Average of 10 percentages, 10 transmission data to train, 10-transmission data to test, diagquadratic
 Average of 10 percentages, On-Off data to train, 10-transmission data to test, linear	 Average of 10 percentages, On-Off data to train, 10-transmission data to test, diagquadratic

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

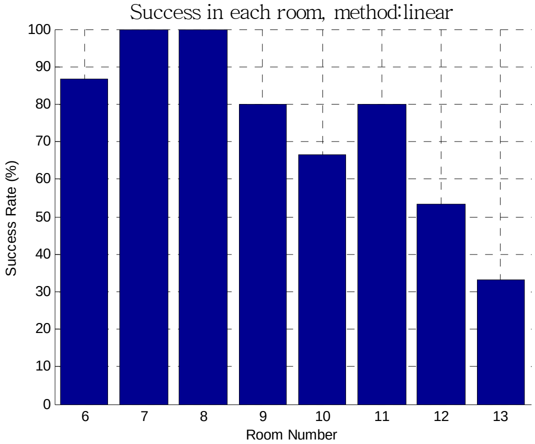
Relaxed sense successful rate of each room is shown in the following figures:



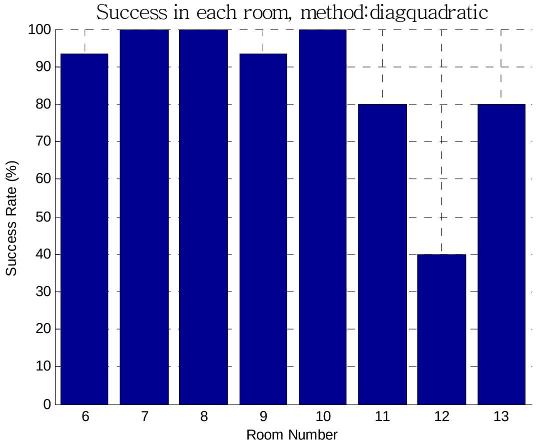
Average of 7 features, 10-transmission data to train, 10-transmission data to test, linear



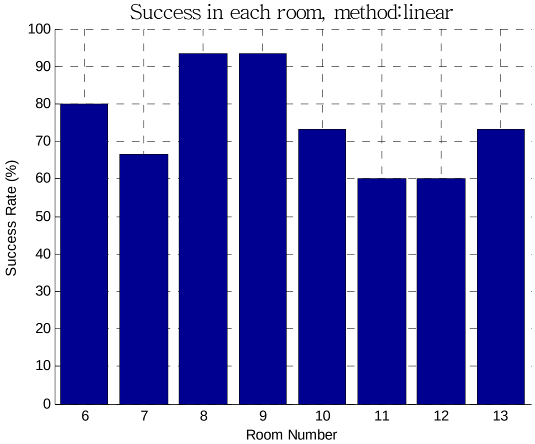
Average of 7 features, 10-transmission data to train, 10-transmission data to test, diagquadratic

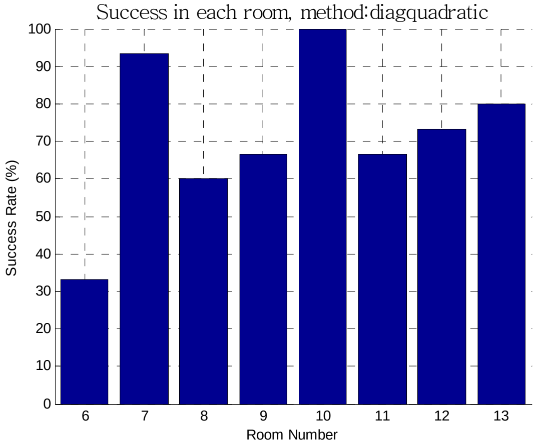


Average of 7 features, On-Off data to train, 10-transmission data to test, linear

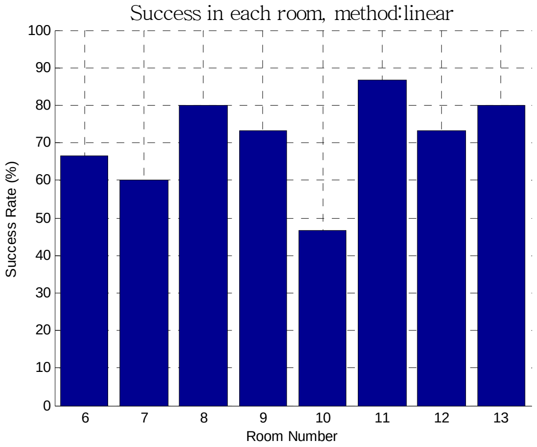
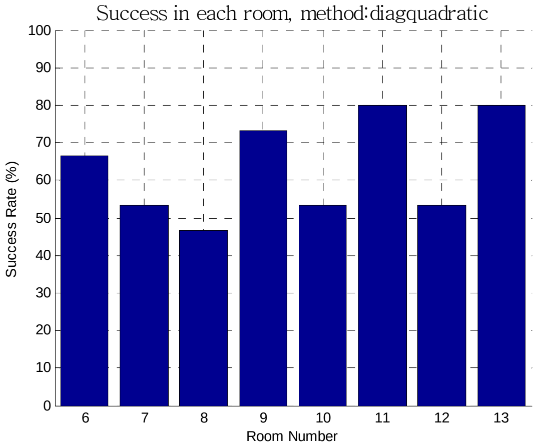


Average of 7 features, On-Off data to train, 10-transmission data to test, diagquadratic





This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

Average of 10 percentages, 10-transmission data to train, 10-transmission data to test, linear	Average of 10 percentages, 10 transmission data to train, 10-transmission data to test, diagquadratic
 Average of 10 percentages, On-Off data to train, 10-transmission data to test, linear	 Average of 10 percentages, On-Off data to train, 10-transmission data to test, diagquadratic

5.7 Tests with Volunteer Cellphones

Our hardware is built to capture any CDMA cell phone signals. The final demonstration must take place with actual cellphones, not with modem powered off. Thus, we randomly called for 6 Verizon CDMA cell phone holders as our volunteers. In these experiments, each volunteer is asked to use the cell phone near Antenna 1 and in the office. We found the hardware has different sensitivity to different cell phones, but all the cell phone signals are captured by the hardware. At the same time, we did some experiments during normal business hours. A couple of cell phone transmissions were captured. Based on the volunteer cell phone channel information and the data we collected in 21 rooms, we are able to locate the specific person who is using the cell phone. However, more volunteer tests and data collection are needed to improve the final demonstration.

5.8 Tests with Prepaid Cellphones from Three US Carriers

As mentioned earlier, we bought prepaid cell phones running on different networks (850MHz CDMA2000, 1900MHz GSM and WCDMA, 1700 MHz GSM and WCDMA). Each prepaid cell phone is tested in the same manner and scenarios as that of CDMA2000 modem. The prepaid cell phones testing results are actually better than those of modem. Thus, our hardware and fingerprinting approach have been validated by cell phones experiments.

5.9 Conclusions

Based on all the testing results, we have the following conclusions:

1) The more location points collected in one room, the higher successful rate we can get.
2) For each location in each room, 10 -20 transmissions are enough.
3) The receiver has different sensitivity to different cell phones and different bands.
4) Dia-quadratic classification method always gives us the best successful rate.
5) Signals strength is more reliable and works better than TDOA.
6) To improve the sensitivity of one specific band, adding an LNA is a good option.
7) In the data collection process, cell phone actually works much better than modem, if appropriately programmed.

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

8) More antenna could improve the accuracy significantly, however this increase the system cost significantly

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

6. Tartarus

6.1 Hardware and Software

Towards development of a final product, we name the whole system as Tartarus, shown in Figure 42, and filed a patent which is pending at this time. In this product and patent, 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. During the subject period of performance we also performed extensive testing of the system. Below we briefly report the system parameters. Table 1 shows the specifications for Tartarus.

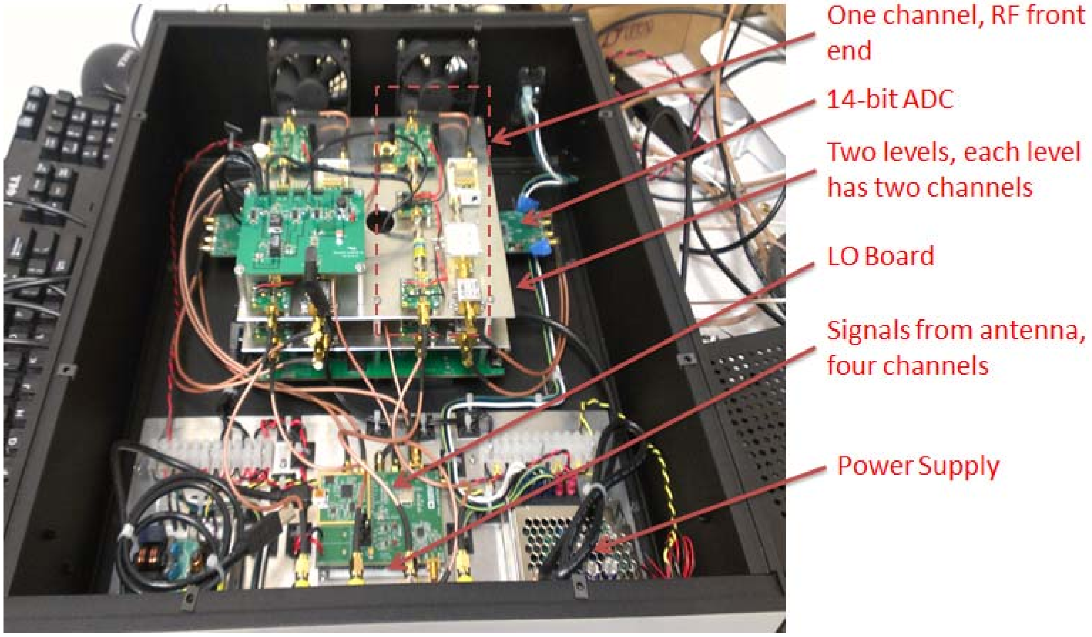

One channel, RF front end
14-bit ADC
Two levels, each level has two channels
LO Board
Signals from antenna, four channels
Power Supply

Figure 42: Tartarus internal hardware and enclosure

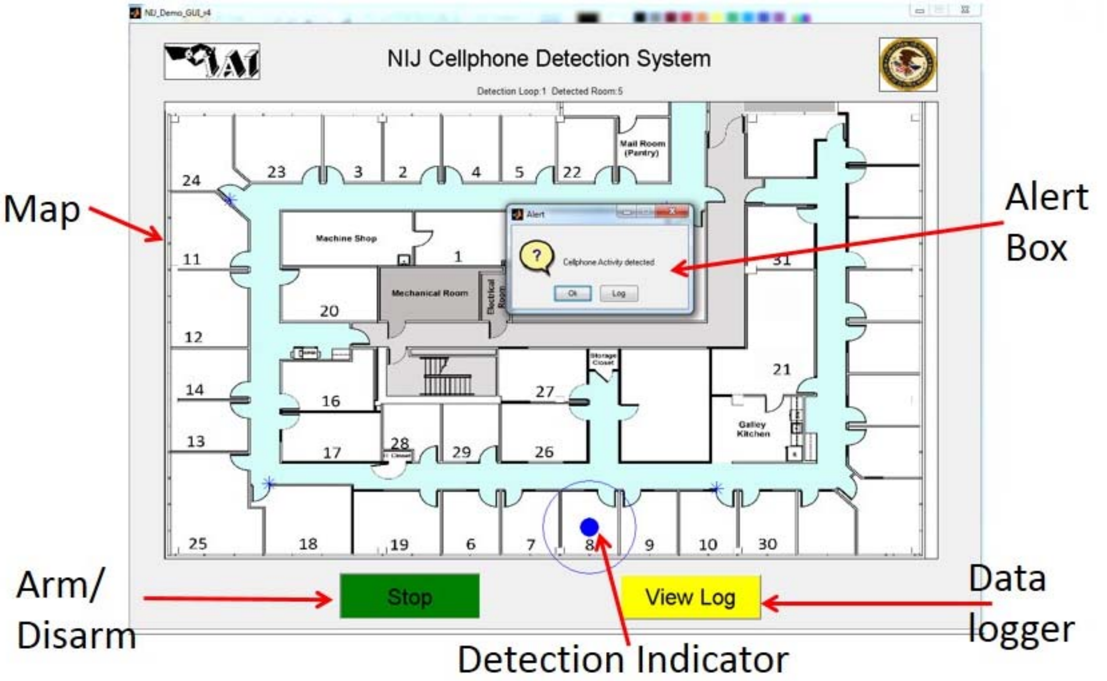
Table 1: Tartarus System Specifications.

Weight	**~1lbs**
Size	**24”x 24” x 6”**
Primary Processing Unit	**Virtex 5 LX95**
Power consumption	**~20W**
Mounting	**Antennas mounted on inner walls**
Area covered with 4 antennas	**~80ftx60ft**
Max. antennas per system	**4 (could be extended to 16)**
Band Coverage: 850MHz, 1700MHz, 1900MHz	**Verizon CDMA, AT&T GSM and WCMDA, and T-Mobile GSM; (LTE bands could also be covered by changing LO and frond end BPFs)**

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

Location Accuracy	**+/- 1 room**

Based on feedback from Harris Corporation and internal review, several improvements were made to the user interface (Figure 43). A map of the monitored area, marked with office numbers is provided. A button to arm/disarm the system is provided. A visible detection alert, along with a data logger is provided. A detection indicator, whose color is dependent on level of confidence, is provided at the estimated position of the cell phone.


NIJ_Demo_GUI_r4

NIJ Cellphone Detection System

Detection Loop:1 Detected Room:5

Alert

Cellphone Activity detected

Figure 43. Graphical User Interface.

A pop-up window allows the Insertion of user comments at the time of detection (Figure 44)

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

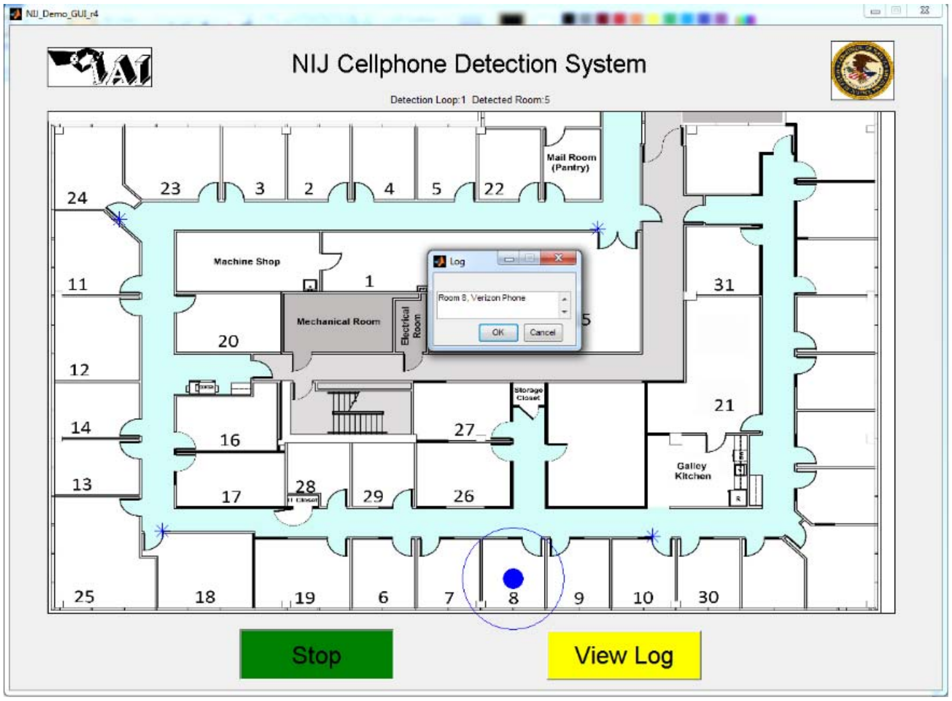
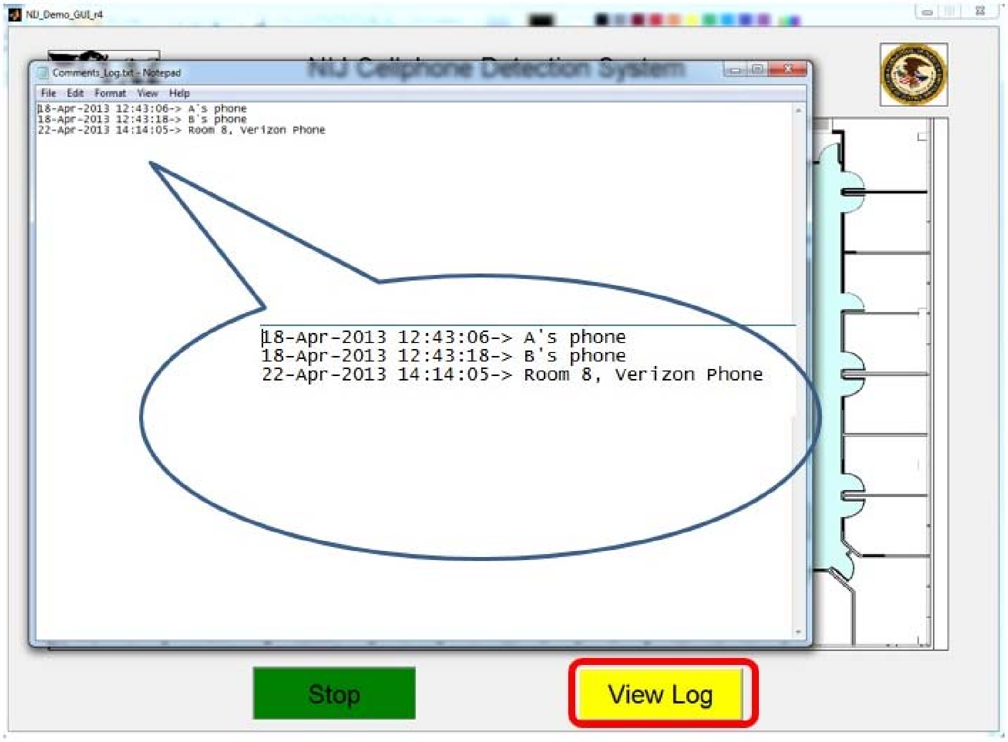


Figure 44. Insertion of user comments at the time of detection.

Logged events can be retrieved during run time (Figure 45).


NIJ_Demo_GUI_r4
NIJ Cellphone Detection System
Comments_Log.txt - Notepad
File Edit Format View Help
Stop
View Log

```
18-Apr-2013 12:43:06-> A's phone
18-Apr-2013 12:43:18-> B's phone
22-Apr-2013 14:14:05-> Room 8, Verizon Phone
```

Figure 45. Log file is retrievable in runtime,

Extensive data was taken in every room of the test area (west wing of IAI office Space, Figure 46). In each room, 15 positions were selected. From each position up to 50 transmissions were recorded.

This process was repeated several times to test repeatability and stability of the system. Each room calibration took approximately 30 minutes (if everything went smoothly), and was performed at night to reduce the effect of other cell phone activity, and movement of people and/or equipment during the day.

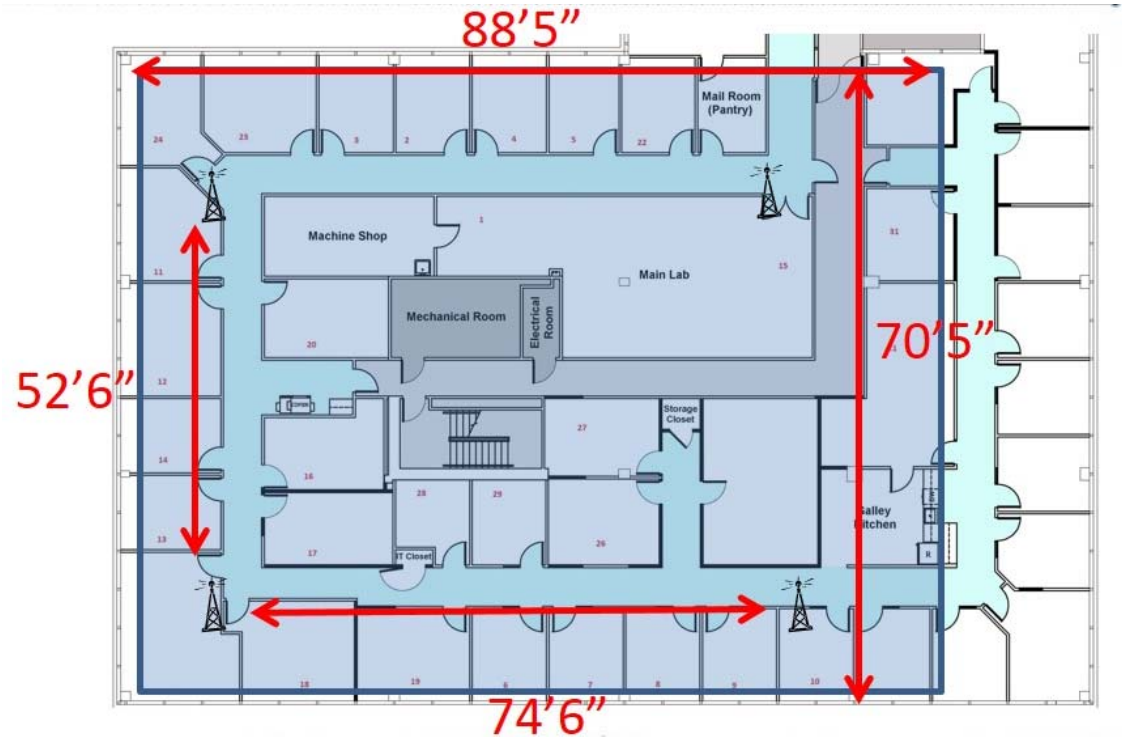


Figure 46. Current Test Area - West wing of IAI office Space.

6.2 Estimation of Maximum Area Covered

We also estimated what the maximum monitored area could be for the current hardware. Our approach is to determine how fast the signal power decays away from the transmitting cell phone, and extrapolate (by fitting a power law to the data) at what distance the received power leads to such low SNR, that detection cannot be guaranteed. We show an example such a graph below in Figure 47.

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

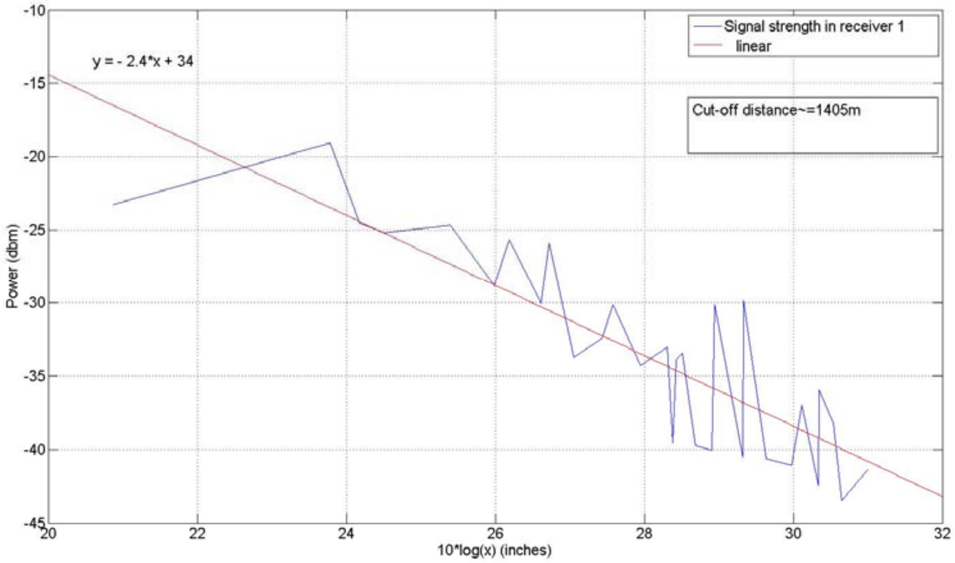


Figure 47. Received power in dBm vs. distance in inches.

In the table below we show estimates of the cut-off distance.

Table 2. Propagation loss (power law exponent obtained from fitting) and estimated cutoff distance.

Propagation Loss	Cut-off distance (m)
2.2	3799
2.4	1405
2.8	294

These estimates suggest that the current system could be scaled up considerably (at least an order of magnitude larger area by placing antennas further apart, thus reducing system cost per monitored unit area or cell by a similar amount.

6.3 Algorithm Optimization

In transition to a final product, we also optimized the system performance by tweaking the algorithms. For review, a high-level overview of the algorithm is provided in Figure 48. The algorithmic approach consists of a calibration phase which contains: signal detection and acquisition, feature extraction, outlier removal, and training of the detection and localization algorithms. This calibration phase leads to a data base containing a RF finger print consisting of 7 features for each room. During operation of the system, signal detection and acquisition, as well as feature extraction remains the same, but are now followed by a classification step (which matches the features to the closest finger print in the data base) , and reporting to the user interface.

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

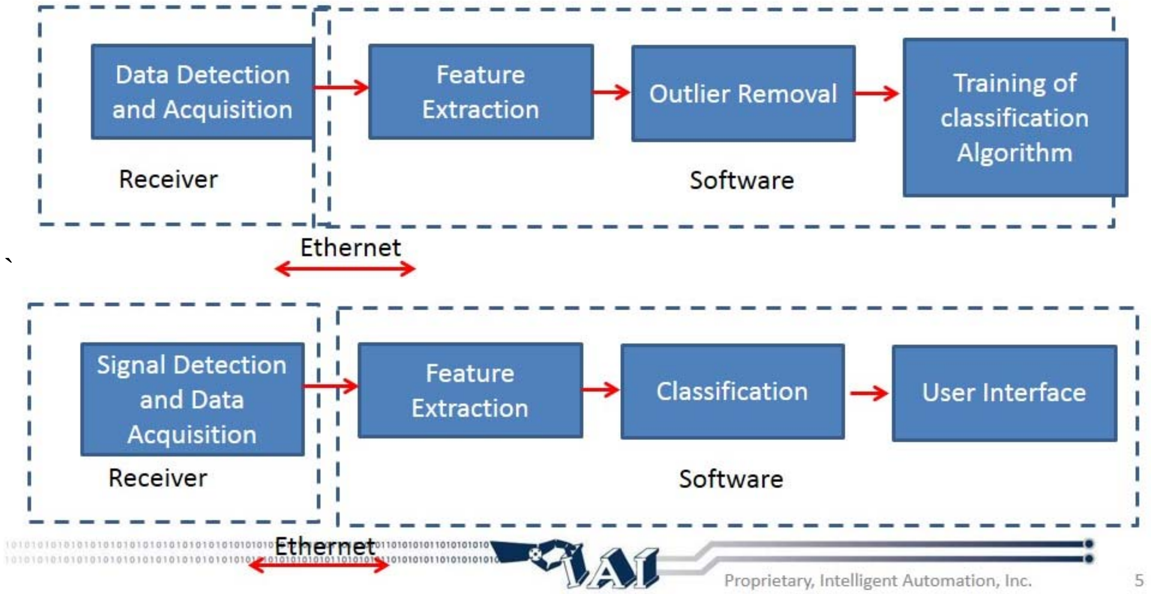

Data Detection and Acquisition
Feature Extraction
Outlier Removal
Training of classification Algorithm
Receiver
Software
Ethernet
Signal Detection and Data Acquisition
Feature Extraction
Classification
User Interface
Receiver
Software
Ethernet
Proprietary, Intelligent Automation, Inc.
5

Figure 48. Algorithm block diagram.

Specifically we explored ways to treat signal strength features differently from TDOA features in the localization algorithms. We found that limiting the search space for a match to rooms that are near the antenna with the strongest received signal works well, when the received signal is above a certain threshold. We show the pre-demonstration results below in Figure 49. Specifically, we denote the posterior probabilities we obtain from the classification algorithm. If it is projected that room *i* is sending information with probability>2/3, we color room *i* green. If it is projected that room *i* is sending information with probability<1/3, we color room *i* red. Otherwise we color room *i* yellow.

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

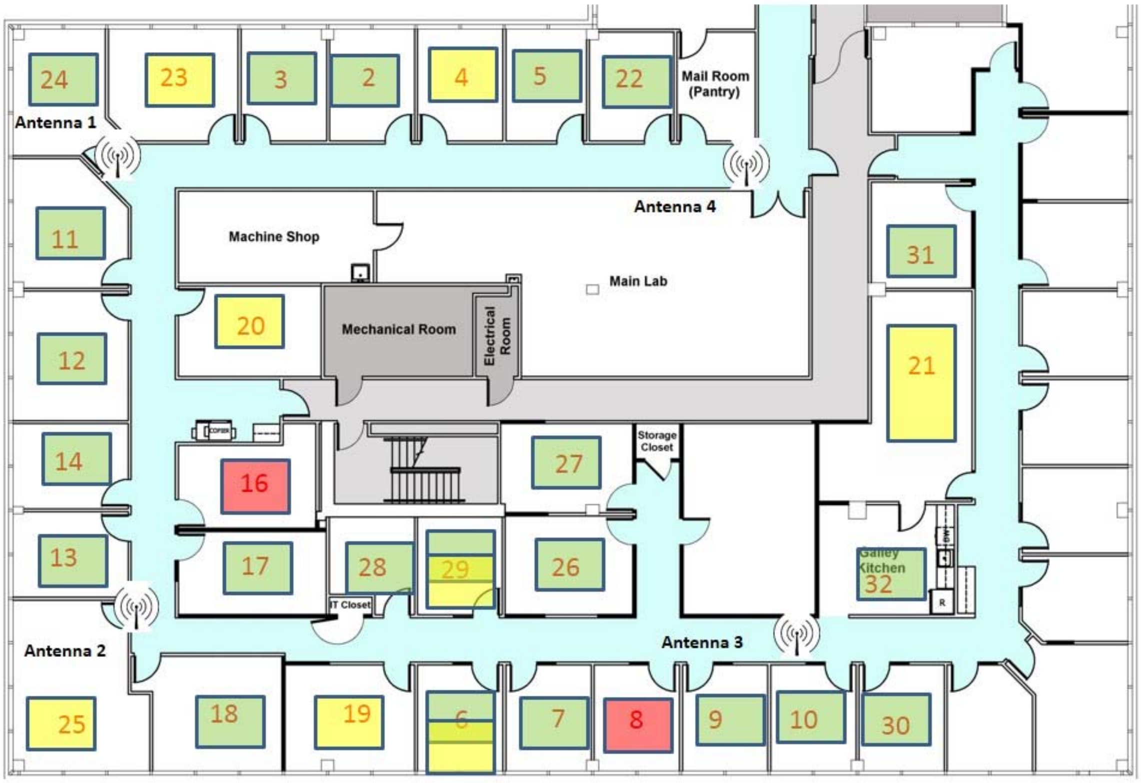


Figure 49. Localization accuracy map.

6.4 All US Cell Phone Band Coverage

During the period of performance, we performed additional testing and hardware modifications in order to complete demonstration of detection and location capabilities for all three US cell phone bands (850MHz, 1700MHz and 190MHz). Testing was performed in the same section of the IAI office as before (Figure 50). Because the energy detection method we used in receiving the cell phone signals, switch to another cell phone band is easy and quick by changing the front end RF BPFs and LO. This process takes about less than 5 minutes.

We show successful localization (+- 1office) for each of the three bands (for a single call or text made by the phone to be detected or localized), Figure 51. We note that the success rate for the 1900MHz and 1700MHz match or exceed those for the previously demonstrated 850MHz band.

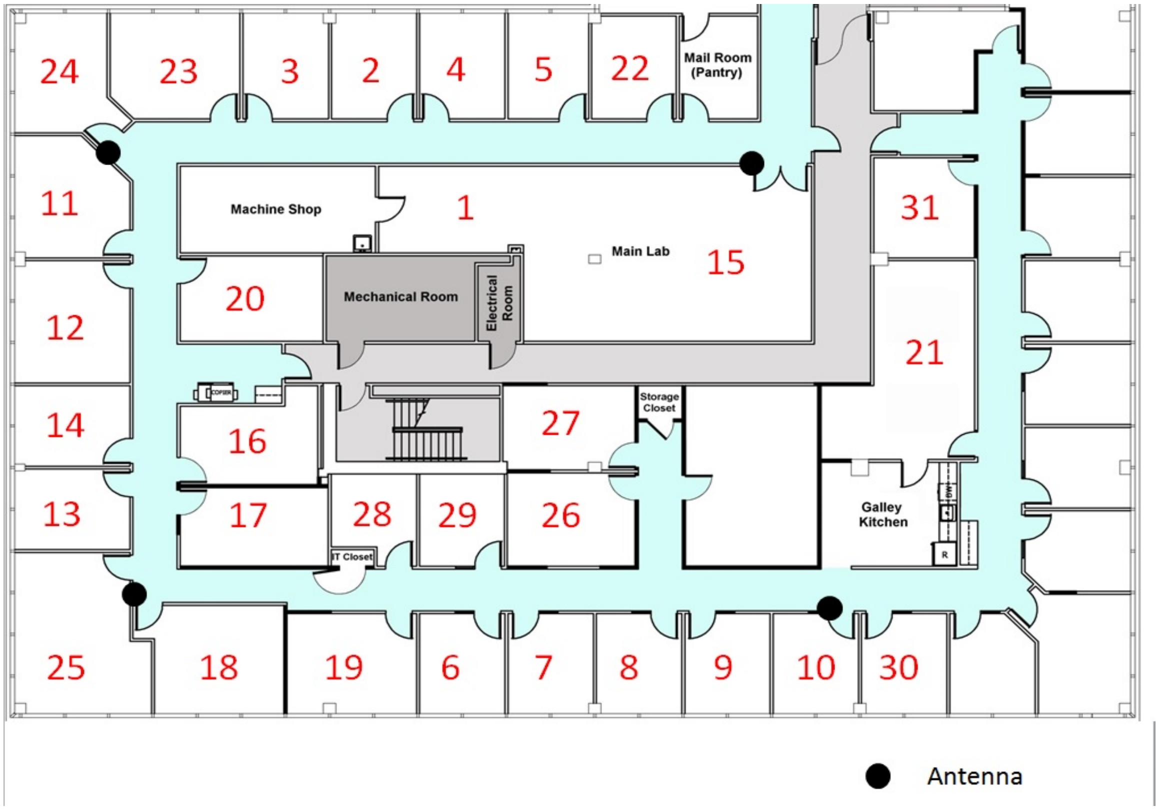


Figure 50. IAI floor plan and room number, for testing and demonstration.

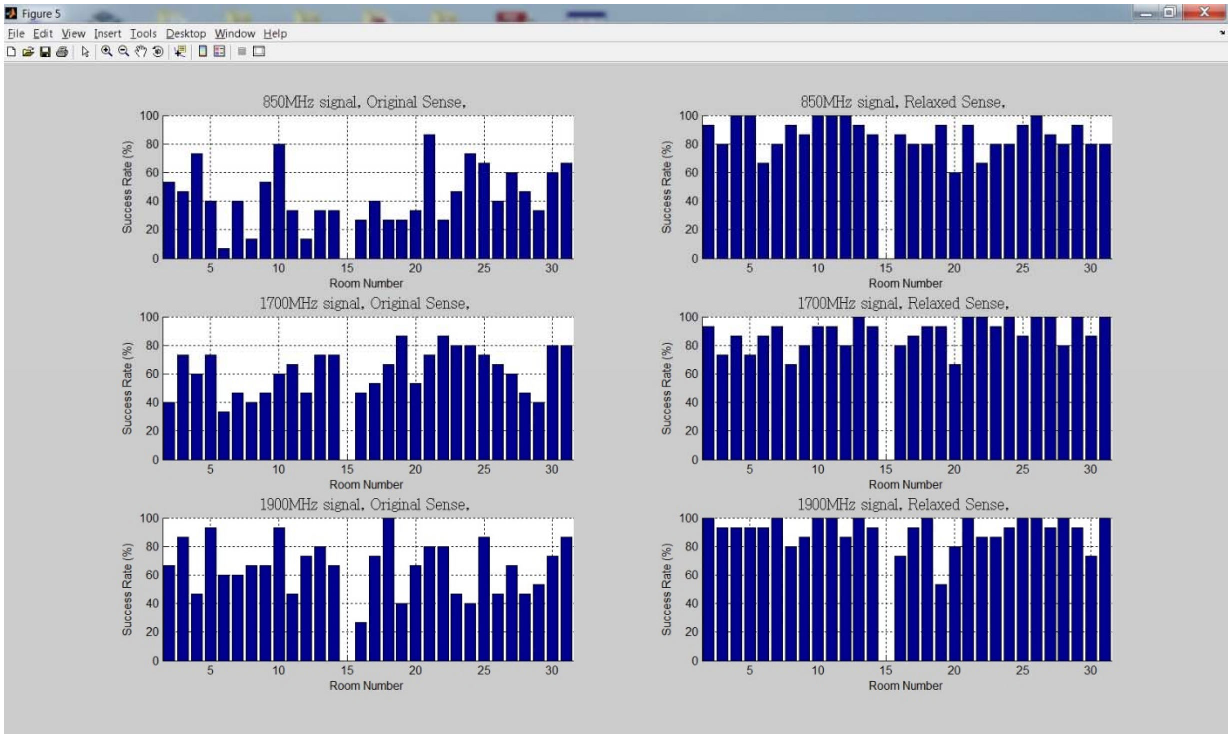


Figure 51. Successful detection and localization rate vs. room number for all three US cellular bands.

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

6.5 Demonstration to NIJ

On April 29th, 2013, the Tartarus system was demonstrated to Dr. Francis Scot form NIJ, and several staff from the Harris Corporation. The demo was performed at 7pm at night. In order to reduce spurious cell phone activity, staff and cleaners were asked to leave before the demonstration.

While the hardware was located in the RF lab (Room 26 in the map), the system was controlled and GUI was displayed in in conference room A, Next we turned the system on. We explained the GUI. And then we armed the system. The COTR and Harris staff took one of three cell phones (AT&T, Verizon and T-Mobile) to a random room of their choice (one at a time). Once in room, they closed the door, and turned on the phone. Next they called conference room A using internal line, reported what room they are in.

And ended the call Next, they turned the phone back on and texted from same room, and used the office phone to report to conference room that they sent a text. Next, they turned off the cell phone, waited a few seconds and moved to another room.

This went on for about half an hour. All text was reliably detected and located. Only a few phone calls were miss-located, among all were detected. Experiments under relaxed conditions, like not turning the phone on/off, and a brought-in Verizon cell phone phone were successful as well.

6.6 Estimation of System Cost

We also prepared a rough cost estimate based on the Bill of Materials (BOM), assembly cost, and installation and calibration cost. Other costs such as documentation, training, warranty, marketing, and profit are not included.

We currently estimate the hardware cost: to be approximately $13K (BOM and assembly). We estimate that these costs could be lowered by reengineering to about $10K. Installation costs were estimated based on the cost of installing coaxial cables in buildings: "Deployment costs: High quality and low attenuation coaxial cabling can cost up to $4.50 per foot for materials and installation because it requires specialized expertise. It is difficult to install because it's heavy and does not bend easily. Standard cabling (fiber & Cat 5) costs about $1 to $2 per foot, including installation" [1]

For 100ft by 100ft area requires approximately 100ft + 100ft + 140ft of cable= 340ft@$3.50/ft = $1200. This a low estimate, longer cables may be needed to rout around obstacles, and added cost may occur due to the hostile environment.

As for overall system cost, these estimates inform an overall system cost estimate. For a 4ft wide cell, and cells along two or three walls, this corresponds to 50/75 cells. For 100 cells, system cost would be $28K.

[1] http://searchnetworking.techtarget.com/feature/In-building-wireless-Installation-issues-trump-equipment-costs

6.7 Operational tasks to be performed by practitioner if technology were commercialized and adopted

In this section, we describe what operational tasks that would be required, from a practitioner's perspective, if a system like this were to be commercialized and deployed. The three main tasks are Installation, Calibration, and Maintenance.

1. Installation

   The installation phase requires running of RF cables or fibers (If RF over fiber is used) outside the cells, and placement of several (about 4) antennas every 100 cells or so. Different levels may need separate antenna and cable runs. Cables/fibers, and antennas need to be not readily accessible to inmates, so the ceiling may be the most appropriate location. In this installation phase, no access to the cells will be needed. We anticipate that for a building containing 300 inmates this installation would be accomplished in a few days. The receiver hardware would be located in an area where guards would be able to operate it. A dedicated computer could be used to display the alerts, or an existing computer could be interfaced to the cell phone localization system, and upgraded with product software

2. Calibration

   The calibration phase requires a survey of each cell to transmit cellphone signals from that location. The survey would take a few minutes per cell, and can be conducted with or without the inmate present in the cell. Several buildings with a few hundred cells could be surveyed in a single day. After the calibration data has been collected, the data would be processed by the contractor. Performance issues would be identified at this point, and may lead to recommended changes in the hardware configuration (add or move antennas). The calibration phase could be completed in a week or less.

3. Maintenance

   The RF signatures of each location will change if significant changes are made to the environment, such as new construction, or significant rearrangement of the interior of cells. The performance of the system should be checked periodically (say annually) by transmitting cellphone signals from a few cells. This maintenance can be accomplished in less than half an hour a year. If the measurements indicate that significant changes in RF signals has taken place, a new calibration may have to be conducted.

7. 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.

8. Participants & other Collaborating Organizations

We provide an overview of IAI staff that contributed to the project in **Table 3** below.

Table 3. IAI project staff.

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

	Project Role	Contribution to project	Other support	Months
STEVENSON, MARK W.	Sr. Mechanical Engineer	Enclosure design and manufacture	Army, ONR	0.1
MORANA, MINERVA	Software Engineer	GUI/Software Development	Army	0.2
BHAT, ARVIND	Sr. Electrical Engineer	Hardware Development	Air Force	0.6
GOMES, JOHN	Electrical Engineer	Data acquisition	Army	0.2
DEY, BISWADIP	Intern	Algorithm design	None	2.1
SMITH, WALTER	Mechanical Engineer	Enclosure design and manufacture	Army, Navy	0.1
LIN, CHUJEN	Group lead	Review	ONR, DARPA, Air Force, Army, IAI Overhead	0.2
SCHWARTZ, JOSEPH E.	CEO	Review	IAI Overhead	0.1
VAN DOORN, ERIC	PI	System design, algorithm design	ONR, DARPA, Air Force, Army	1.0
CHEN, PETER		Transition	Army, Air Force	0.1
LONSKE, BENJAMIN	Sr. Electrical Engineer	System development	Navy, Army	0.2
GADDAM, SIDDHARTH	Electrical Engineer	Firmware development	Air Force, DHS	1.4
HOVARESHTI, PEDRAM	Sr. Electrical Engineer	Data acquisition and processing	Navy, DHS	2.7
GUO, ZHITONG	Electrical Engineer	Data acquisition and processing	DOT	6.5

Total				15.6

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

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

9. 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.

10. Changes/Problems

“Nothing to Report.”

11. Budgetary Information

“Nothing to Report.”

12. Conclusions and Future Work

Our extensive study and experiments have shown that we can reliably detect and locate the CDMA, GSM and WCDMA cellphone emitter in the IAI office setting with an accuracy of +- 1 office, using recordings obtained over less than 1 minute of phone use. The transition from prototype to product has been in process. We are also actively looking partners and collaborators in making the final products available in the market.

Future work includes:

1) Perform extensive experiments in outdoor environment, based on the existing hardware.
2) Perform demonstrations in prison environment.
3) Integration the BPFs for three bands so that user does not need to switch bands manually
4) Redesign the system hardware and software to make it more affordable.
5) Explore LTE band and potentially cover LTE cell phone signals.

This document is a research report submitted to the U.S. Department of Justice. This report has not been published by the Department. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.