U.S. DEPARTMENT OF ENERGY

PNNL-17734

Prepared for the U.S. Department of Energy
under Contract DE-AC05-76RL01830

Cell Phone Detection Techniques

RM Pratt
KJ Bunch
DJ Puzycki
RW Slaugh
MS Good
DL McMakin

October 2007

Pacific Northwest
NATIONAL LABORATORY

DISCLAIMER

PACIFIC NORTHWEST NATIONAL LABORATORY
operated by
BATTELLE
for the
UNITED STATES DEPARTMENT OF ENERGY
under Contract DE-AC05-76RL01830

Printed in the United States of America

Available to DOE and DOE contractors from the
Office of Scientific and Technical Information,
P.O. Box 62, Oak Ridge, TN 37831-0062;
ph: (865) 576-8401
fax: (865) 576-5728
email: reports@adonis.osti.gov

Available to the public from the National Technical Information Service,
U.S. Department of Commerce, 5285 Port Royal Rd., Springfield, VA 22161
ph: (800) 553-6847
fax: (703) 605-6900
email: orders@ntis.fedworld.gov
online ordering: http://www.ntis.gov/ordering.htm

This document was printed on recycled paper.
(9/2003)

Cell Phone Detection Techniques

Rick Pratt, Kyle Bunch, Dave Puczyki, Ryan Slaugh, Morris Good, and Doug McMakin

October 2007

Pacific Northwest National Laboratory
Operated by Battelle
for the U.S. Department of Energy
under Contract DE-AC05-76RL01830

Cellular Telephone Detection Techniques

Summary

A team composed of Rick Pratt, Dave Puczyki, Kyle Bunch, Ryan Slaugh, Morris Good, and Doug McMakin teamed together to attempt to exploit cellular telephone features and detect if a person was carrying a cellular telephone into a Limited Area. The cell phone's electromagnetic properties were measured, analyzed, and tested in over 10 different ways to determine if an exploitable signature exists. The method that appears to have the most potential for success without adding an external "tag" is to measure the RF spectrum, not in the cell phone band, but between 240 and 400MHz. Figures 1- 7 show the detected signal levels from cell phones from three different manufacturers.

Recommended Path Forward

We recommend continuing the development of the cellular phone detector using the RF spectrum measurement approach. This approach listens for spurious emissions resulting from the cellular phone when it is either waiting for a call or transmitting. This approach has several advantages including:

1. The detection method is completely passive - it does not require using an external signal to detect the cellular telephone.
2. The band of frequencies identified to detect a wide variety cellular telephones is limited. Since the RF section of a cellular phone must produce a signal within the allocated FCC frequency spectrum, it is likely that manufacturers would not redesign the RF section. Further, a limited number of chip sets used to generate the RF are likely to be used by most manufacturers. Thus, spurious emissions are likely to occur at common frequencies among different models. Further, the fact that the channel frequencies are fixed dictates the oscillator frequency and the multiplier factors in order to generate these frequencies.
3. The system would be flexible to detect more than cell phones. Most active electronics radiates some spurious emissions, and a system could be built to select for particular RF bands. Further, a system could be made to adapt to changes in technology.
4. The system should be useful for many future generations of cellular phones. Manufacturers are required to satisfy FCC minimum spurious power emissions. However, no requirements exist to reduce these emissions to zero, even if this were possible. Because shielding is costly, it is likely manufacturers will continue to design to this minimum requirement and not below. Thus, all cellular phones are likely to have some level of detectable emissions even as technology advances.
5. The system has the potential to detect a cellular phone even when it is turned off. However, this possibility is unlikely. A cellular telephone has some minimal electronics active even when turned off. For example, it is known that a cellular phone can be set to wake up at a particular time; thus, at minimum, a clock must be running. If this electronics produces spurious emissions, it is possible to detect the phone. Additional testing is necessary to evaluate this option to date.

At this point, we have demonstrated that spurious emissions can be detected from several models of cellular phones in the frequency range from 240-400 MHz. We have not performed a thorough analysis of these emissions, nor a thorough study of emissions from different model phones. Further, we have more advanced equipment that can more thoroughly analyze cellular phone emissions than what was available when this project began. Given the potential of this detection method, we propose the following path forward:

1. Perform a thorough spectrum analysis of several cellular phone models. We have a real-time spectrum analyzer that will allow us to perform analyses over a wider bandwidth. We will also be able to detect frequency "hopping" in order to better determine what frequency bands are likely to produce the best detection coverage. This effort will require some Labview programming in order to control the real-time spectrum analyzer. We can further analyze cellular phones when they are turned off to search for spurious emissions.
2. Determine the source of spurious emissions from cellular phones. We have not determined if the emissions we have detected are generated from the computer electronics (i.e., a computer clock chip) or from the RF chain of the phone. We have several cellular phones that have been donated to us that we can carefully disassemble and probe to determine the source of these emissions.
3. Determine the chip sets typically used in cellular phones and the likely spurious emissions generated from these chip sets. We can test a large number of cellular phone models, but we cannot test them all. Thus, if we can determine common electronics among different models, we may be able to reasonably extrapolate as to the likely success rate of this detection method for most models.
4. Perform detection experiments within the most promising bands. Our experiment was performed in a metal box with an antenna close to the cellular phones. In this way, we were most likely to find spurious emissions from each phone. It will be necessary to determine bounds on standoff detection from these emissions. Fortunately, portal detection will require detection distances less than a few meters.
5. Determine hardware requirements for a detection system. A hardware system will most likely have to scan over a frequency range using a sensitive detector with a narrow band filter. Sensitivity requirements, bandwidth requirements, and so forth, will allow us to estimate hardware costs and system feasibility.

Alternative Path Forward

Another potential path forward is also proposed, but will require additional testing to validate. This method involves sending a short RF pulse (within the cellular phone band) and listen for a two responses – the first response is from any RF reflecting material and a second response (slightly delayed) from the cellular phone filters used on all phones. This approach has the potential to detect cellular phones whether they are ON or OFF or transmitting.

Background

Cell phones have become a very popular communication tool and have been used to surreptitiously gather sensitive information (Appendix A). The need to restrict these devices from areas containing protected information has become apparent and requirements have been mandated. These protection requirements have resulted in 100's of security infractions in the national laboratories each year. Savannah River,

Los Alamos, and Oak Ridge have tested and begun installing a low-powered active RF tag called Rubee and a reader in a portal to perform this function. Each cell phone user must attach one of these tags to his cellular telephone. Sandia National Laboratory presented a technology for detecting cellular phones developed using their internal research and development funding. PNNL testing using a similar approach identified some weaknesses in the Sandia approach.

Bechtel-Nevada conducted an evaluation of a representative sample of commercial cellular telephone detectors in 2003. Sandia National Labs also conducted an evaluation of commercial cellular telephone detectors. There summary finding was that *none of the commercial products* was effective in detecting cell phones when they are turned off, or if they are turned on and a phone call is not in progress.

Testing Philosophy

Mobile phones are highly mobile communications devices that perform an array of functions ranging from that of a simple digital organizer to that of a low-end personal computer. Designed for mobility, they are compact in size, battery powered, and lightweight. Most cell phones have a basic set of comparable features and capabilities. They house a microprocessor, read only memory (ROM), random access memory (RAM), a radio module, a digital signal processor, a microphone and speaker, a variety of hardware keys and interfaces, and a liquid crystal display (LCD). The operating system (OS) of the device is held in ROM, which with the proper tools typically can be erased and reprogrammed electronically. For certain models, RAM may be used to store user data that is kept active by batteries; these data will be lost through failure or exhaustion of the batteries. The tests below were designed to detect cellular phones and focusing on the microphone, speaker, and RF system as potential vulnerability entry points.

RF Transmission Technique

Each cell phone was placed in the bottom of a simple metal enclosure with a whip antenna about 4” away. The RF spectrum within the metal enclosure was measured for the duration of the test. In figures 1 – 7 below, the red signals standing alone are frequencies in which the cellular phone could be discriminated from the background signals:

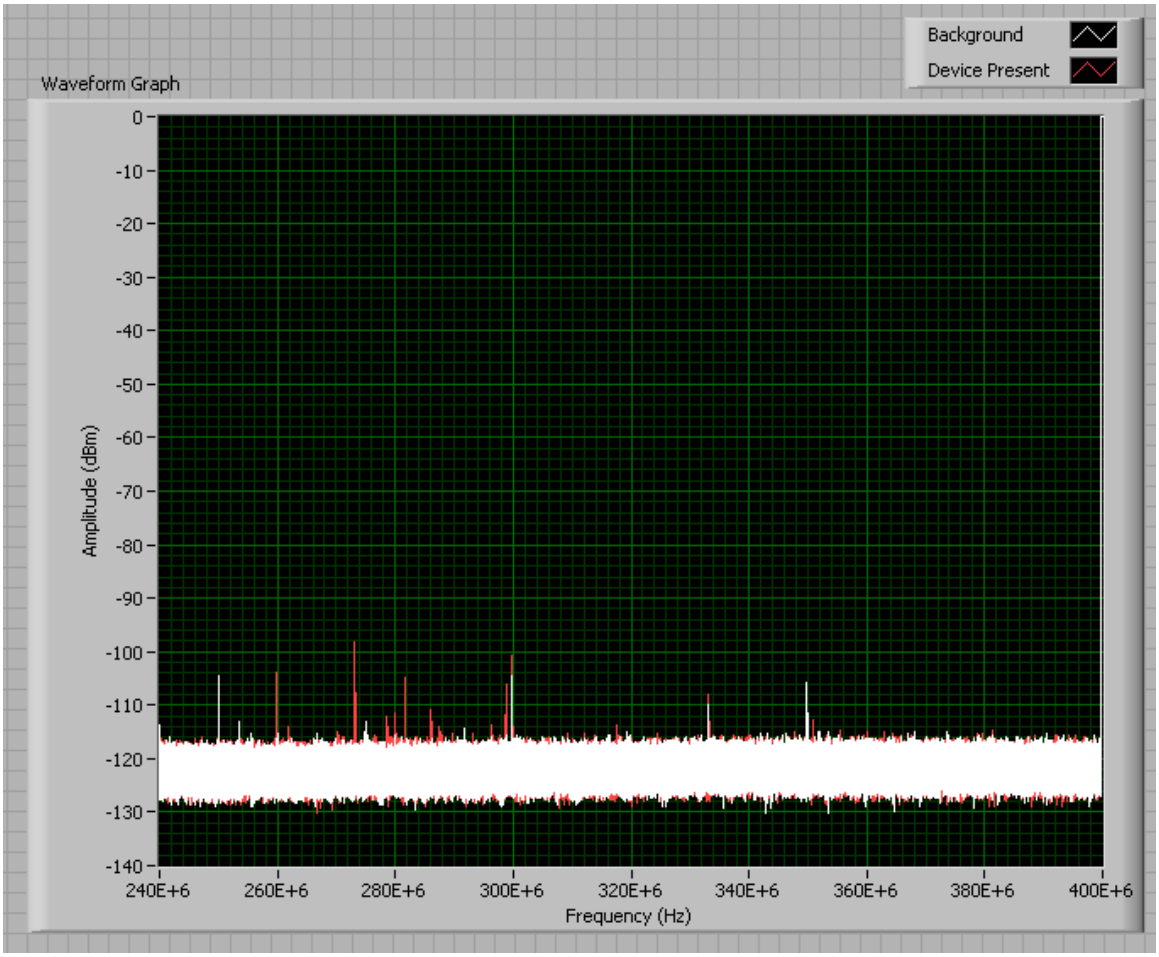


Figure 1 - New LG Cell Phone

The LG cellular phone had distinctive signals from 260MHz to 300MHz.

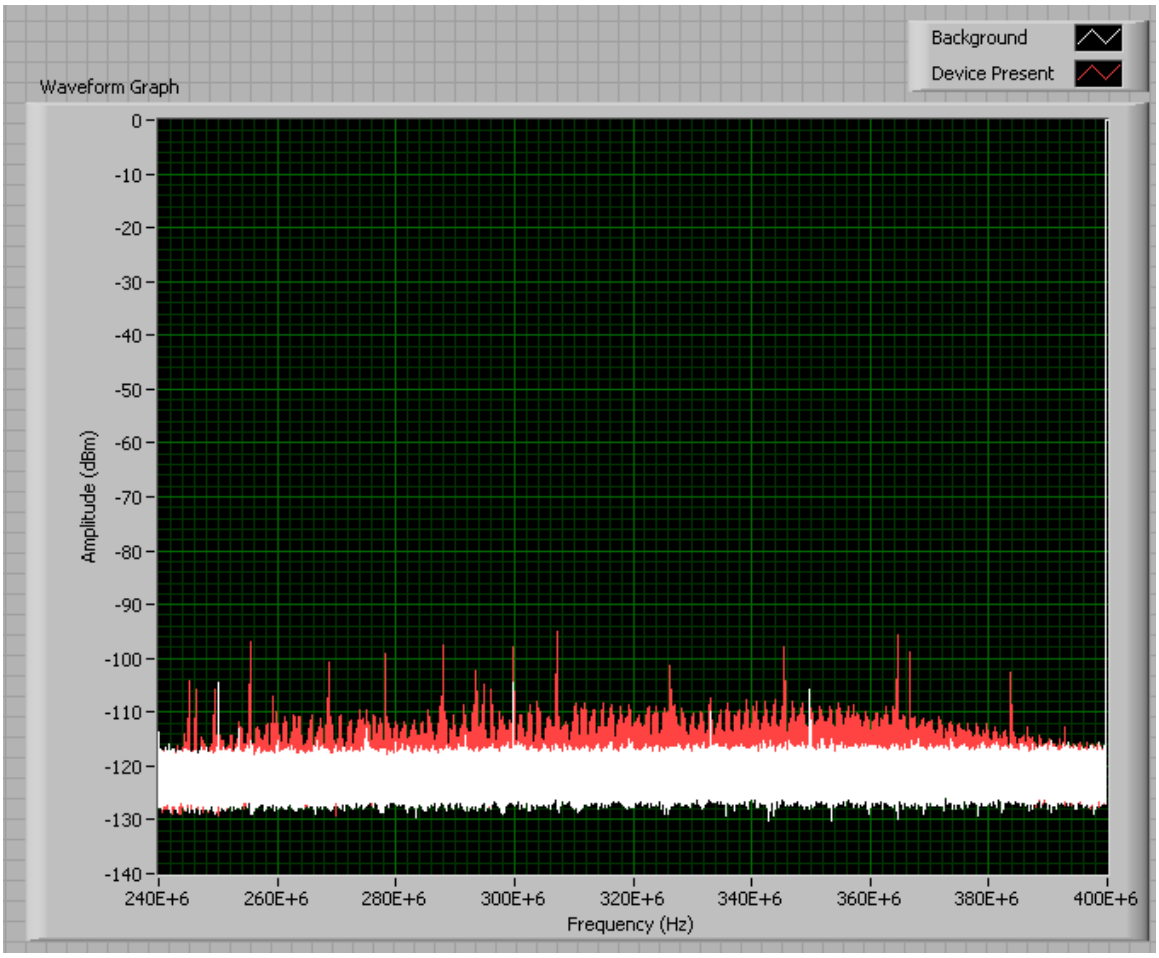


Figure 2 - New Motorola Cell Phone

The Motorola cell phone had distinctive signals over the entire band.

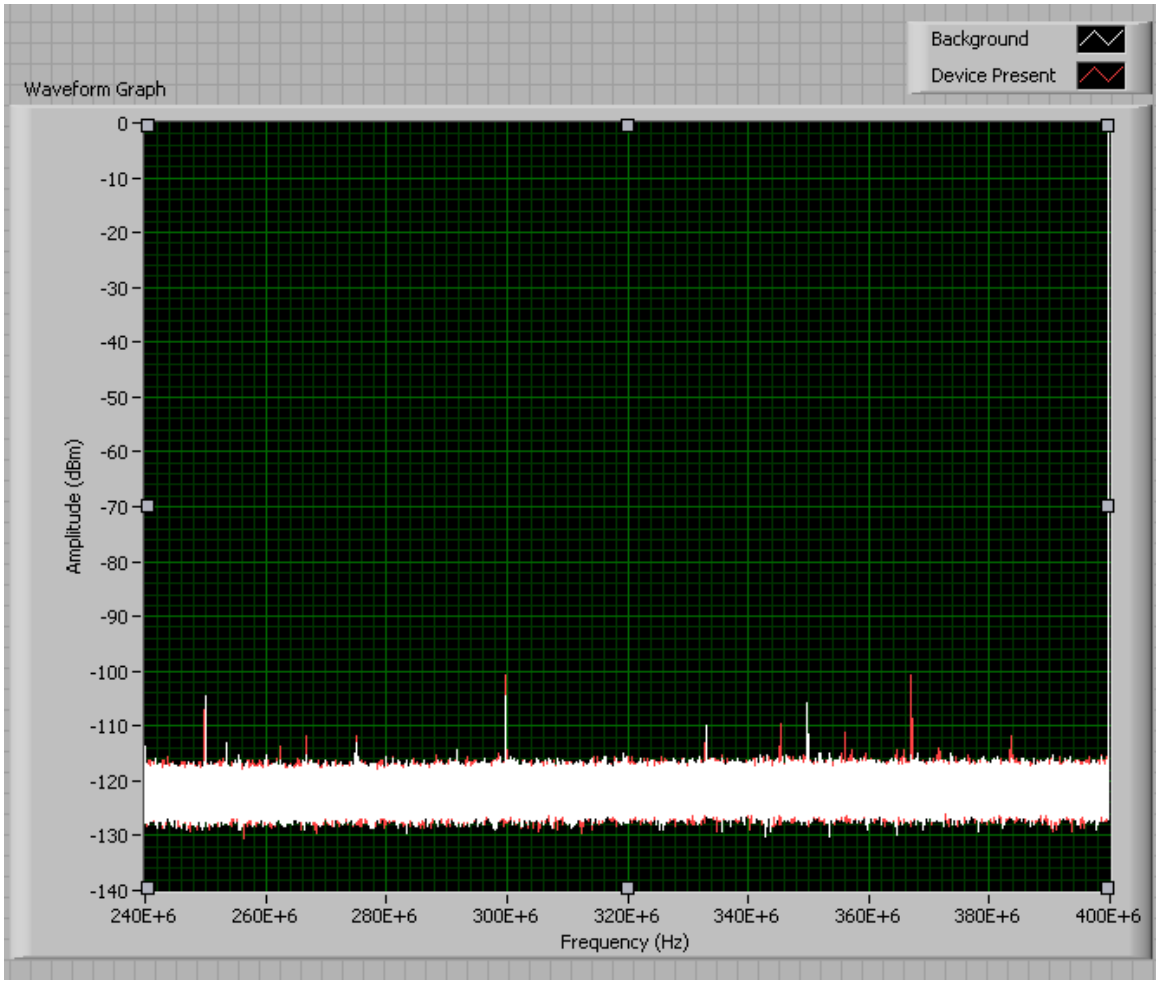


Figure 3 - Old Samsung Cell Phone

The Samsung cell phone had distinctive signals between 340MHz and 385MHz.

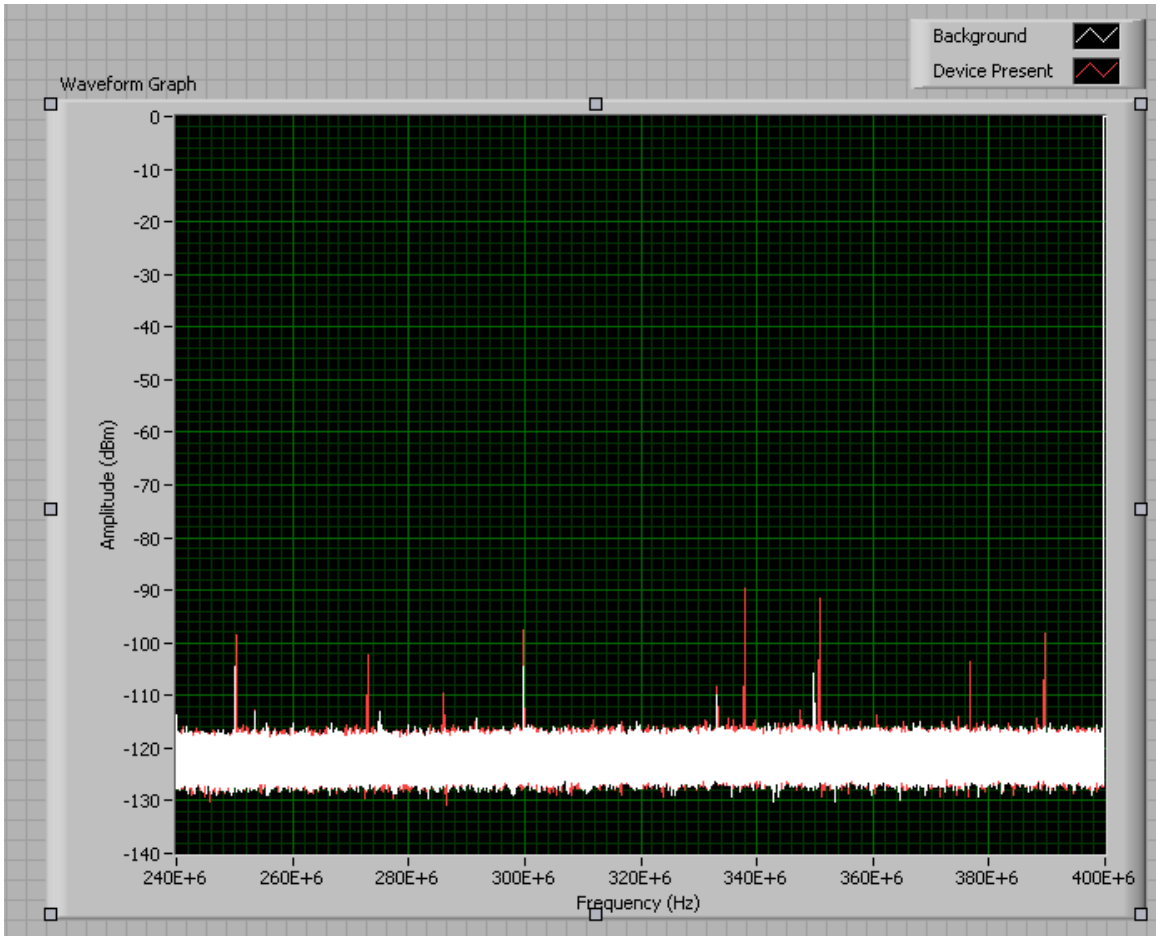


Figure 4 - Motorola 550

The Motorola 550 cell phone had several distinctive signals over the entire band.

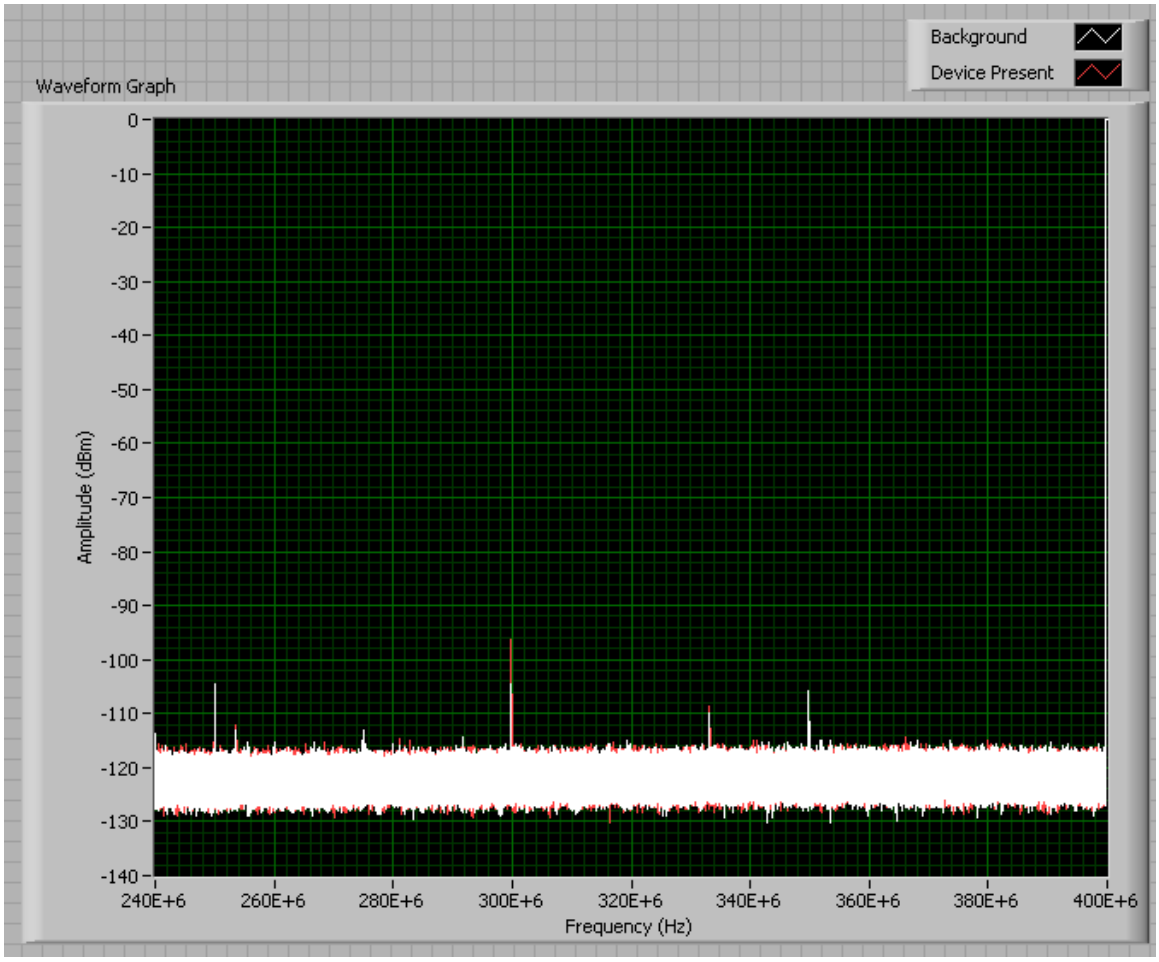


Figure 5 - Iphone

Detecting the Iphone will require additional testing.

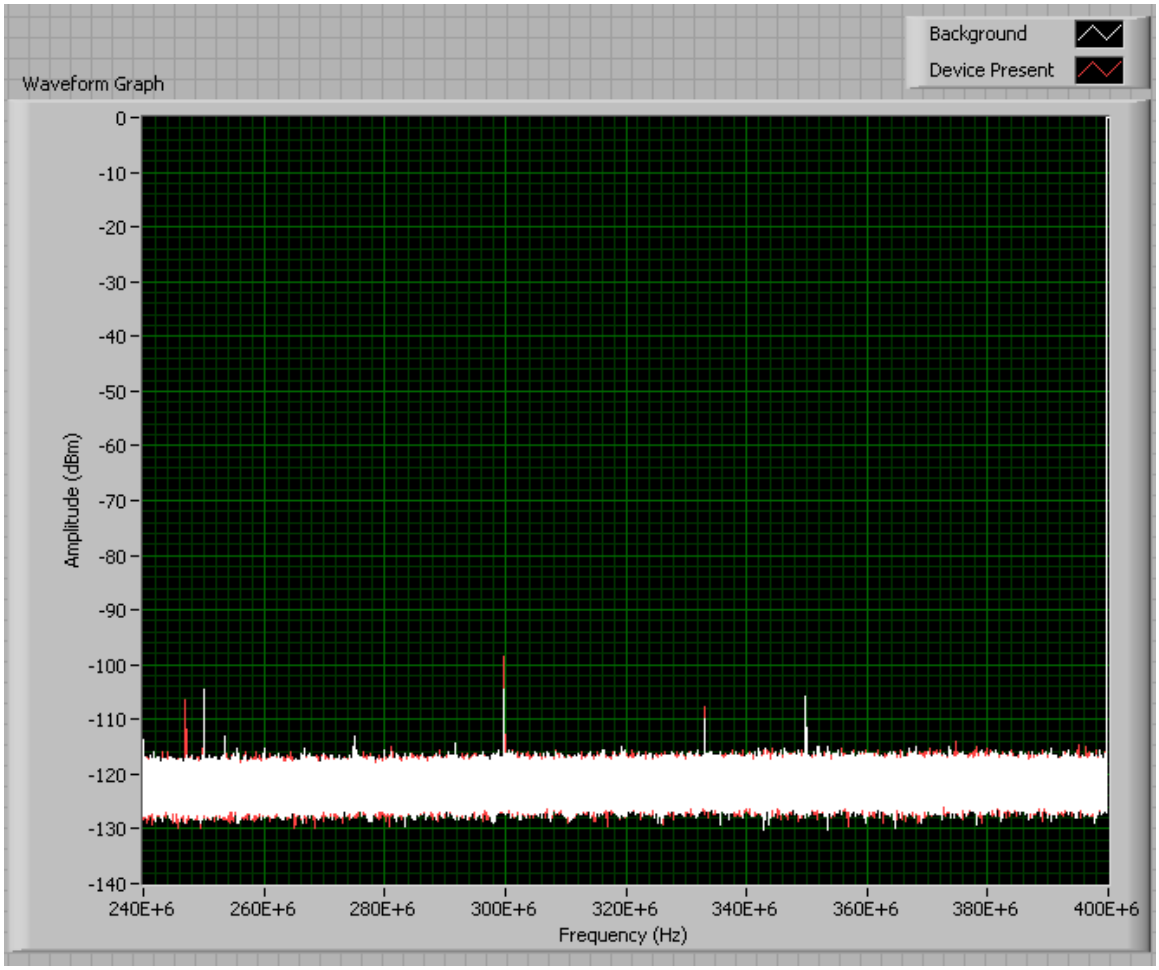


Figure 6 -Older Nokia

The older Nokia has one distinctive signal at 245MHz.

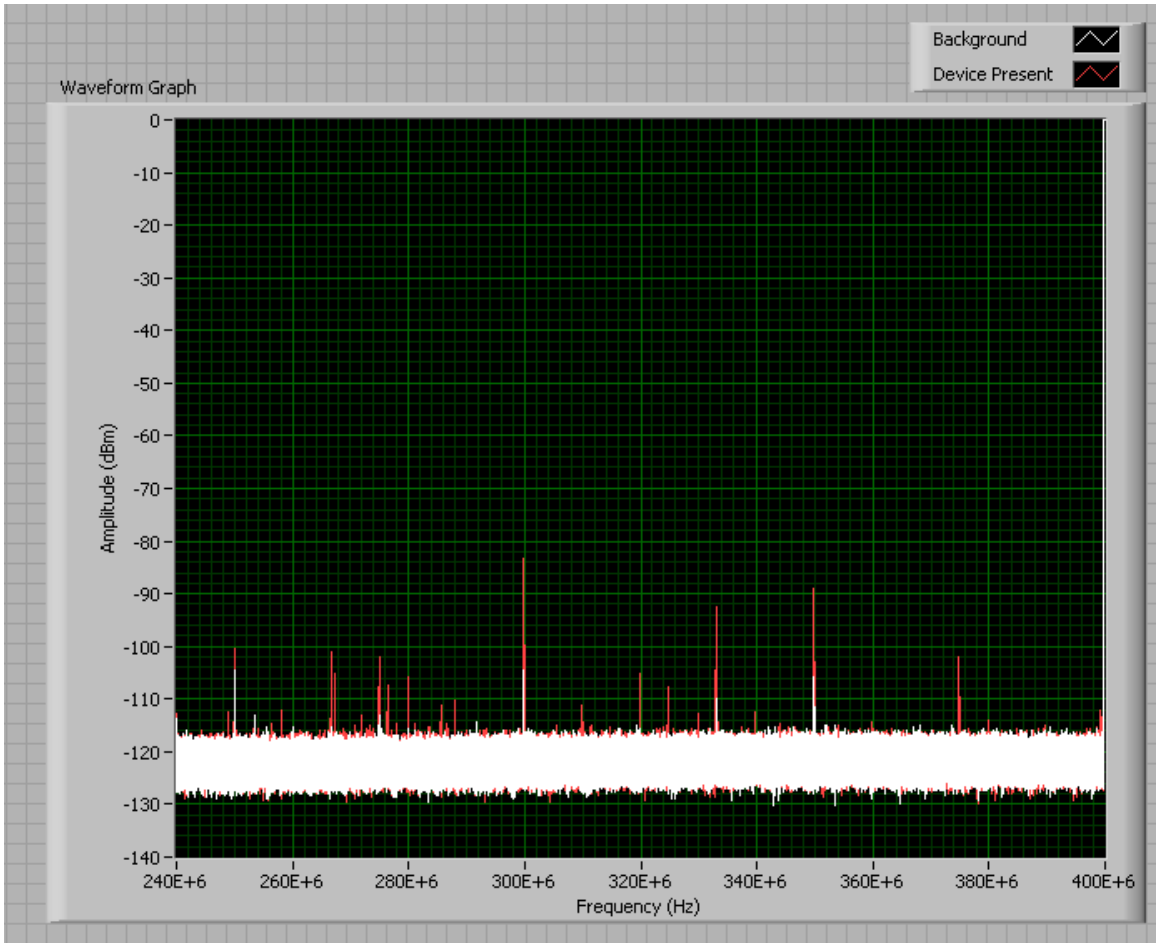


Figure 7 - No Device Lid Open

This scan defines the technical approach that will be required to successfully determine if a cell phone is in the immediate area. The red lines show signals that will need to be masked by the system so that the introduction of a cell phone can be detected. It is proposed that a passive infrared detector be included in the system to detect the presence of a person at the entrance to a limited area. Its function will be to cause the Cell Phone Detector to transition from measurement of the background signals into the cell phone detector mode.

Cell Phone Testing Conducted

Ten methods of detecting cellular phones were conducted – each attempting to exploit a set of cellular telephone features. Cellular telephones actually have two speakers – one for the ringer and one for listening. The ringer speaker has a much larger magnet. A variety of tests were conducted to determine if these magnets could be reliably detected using eddy current instrumentation and "Hall Effect" sensors. Neither of these tests achieved the desired results.

The second effort scanned the RF frequency spectrum around the cellular phone. This test was looking for the internal oscillators necessary to operate the microprocessor and RF synthesizer / mixer. It was obvious from the absence of signal in the RF spectrum that the cellular phone designers had done a very good job meeting the electromagnetic interference specifications.

A third effort involved the use of mm-wave holography and techniques similar to that used by non-linear junction detectors. A sample test setup and image is shown below with red arrows connecting scanned objects to the objects themselves. The cellular phones were OFF in these images.

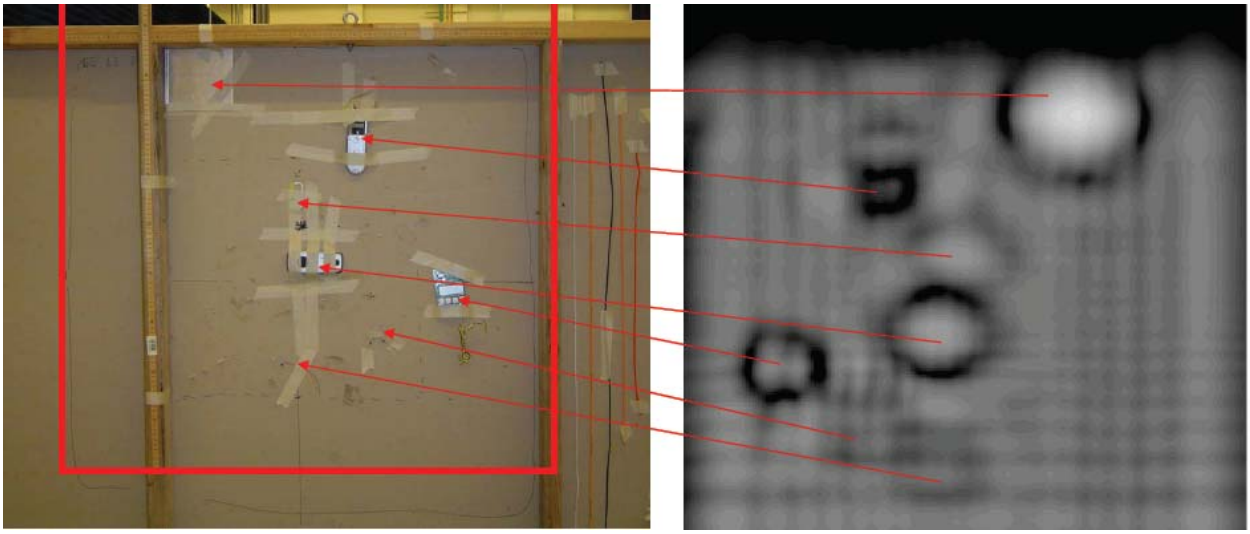


Figure 8 - mm-wave imaging technique

A fourth set of tests involved detecting the transmitted RF from the cellular phone. An "RF Signal Strength" meter was obtained along with an amplifier, mixer, and filter. This technique had no difficulty in detecting the cellular phones as they periodically communicate with the cellular tower. We began to investigate whether or not we could externally initiate the cellular phone to broadcast to the base station, but placed this effort on hold until after the Design Review.

A fifth option was selected. A commercial product was identified from a company called CellBusters. They manufacture a device that continuously monitors for cellular phones, once it detects that a cell phone is switched on (up to 90 feet away) it will alert the phone user that they must switch off their phone. All units are on back order and cost $755 each. The CellBuster, when turned on, will continuously monitor for radio waves emitted from wireless communication devices. The device doesn't transmit and only receives signals, therefore is safe

to use in areas sensitive to Cell phones and two-way radios. The unit can even detect Cell phones hidden in handbags and briefcases. Unfortunately of the 5 reviews written, two units did not work.

The sixth option involved combining RF and acoustic signals to detect the cellular phones. Three sets of tests were performed on 5/23/2007 to determine the technical feasibility of various approaches to identify if a person was carrying a cell phone into a limited area as a result on their oversight. The Magnetic Coupling Test coupled magnetic energy into the cell phone and observing a response. Second Harmonic Test used a modified second harmonic technique where the fundamental frequency was modulated at 3kHz. Combined Audio and RF Test used an audio source and observed the detected RF response.

Magnetic Coupling Test Setup.

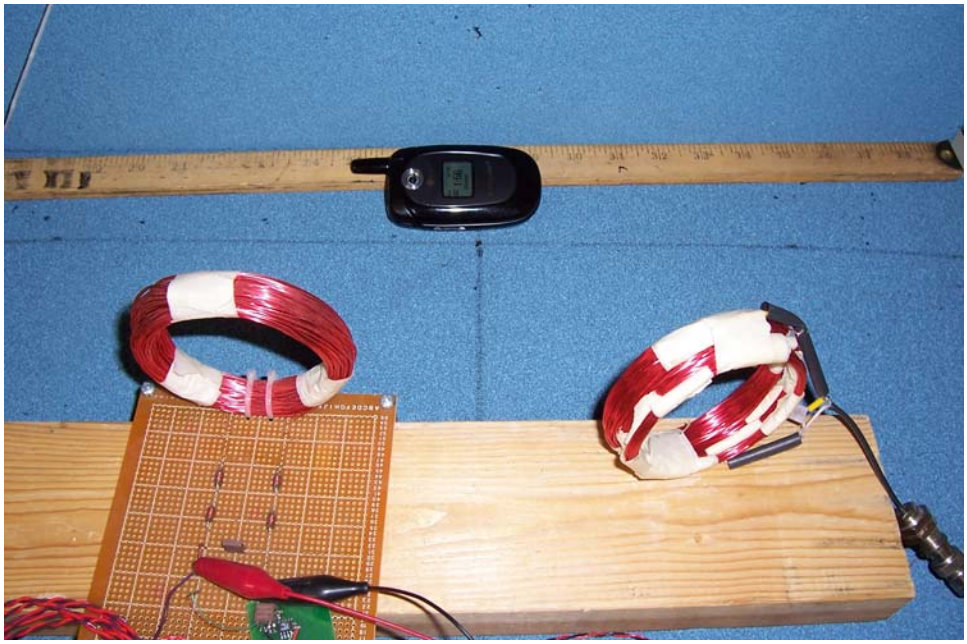


Figure 9 - Magnetic Coupling Test Setup - 28MHz Coils

This test configuration was a frequency synthesizer driving one coil at 28MHz and the spectrum analyzer monitoring the output of the second coil. The cell phone's presence or position relative to either coil made no change in the observed signal from the second coil.

Second Harmonic Test Setup

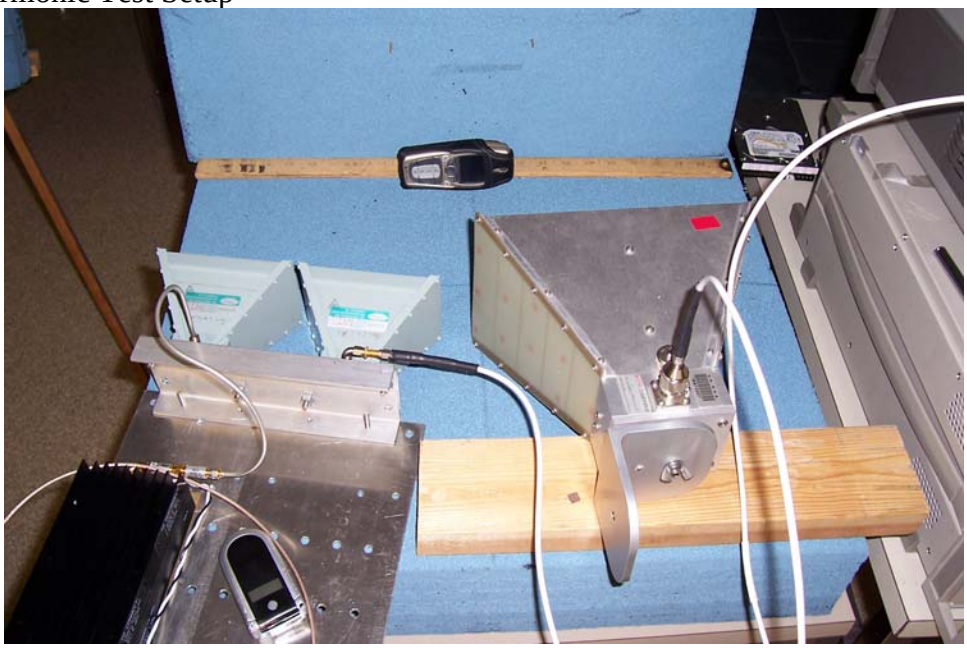
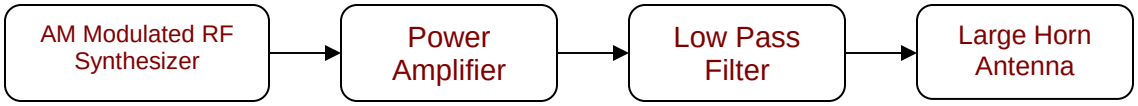


Figure 10 - Second Harmonic Test Setup – Modified Non-Linear Junction Detector

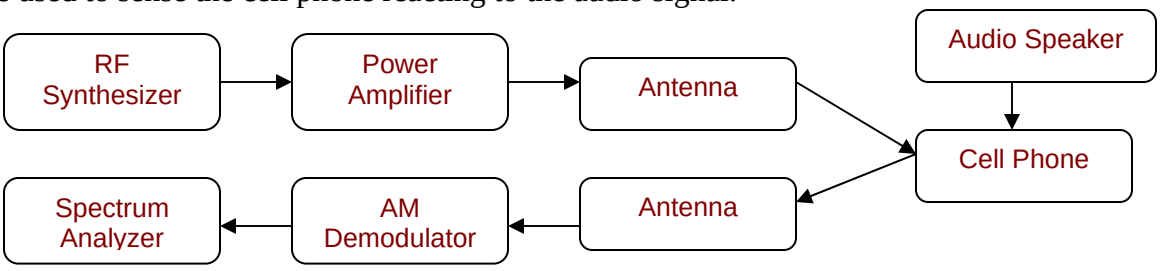
Second Harmonic Test was a modified version of how a non-linear junction detector operates. The horn antenna on the right was connected to two low-pass filters, then a 40dBm power amplifier, and then to a frequency synthesizer. The small horn antenna on the left was directly connected to an RF spectrum analyzer. The RF spectrum analyzer was configured to demodulate AM signals (similar to an AM radio).



Combined Audio and RF Test Setup

Figure 11 - Combined Audio and RF Test Setup – Acoustic Modulated RF Signal

Combined Audio and RF Test replaced the AM Modulated RF Synthesizer used in Test #2 with an RF Synthesizer and removed the low pass filters. (A continuous wave RF signal was used). The horn antenna on the right was connected to a 40dBm power amplifier, and then to a frequency synthesizer. The small horn antenna on the left was directly connected to an RF spectrum analyzer. The RF spectrum analyzer was configured to demodulate AM signals. This test added an audio speaker (located between the antennas) to try to make the cell phone's microphone (or speakers) react to the audio signal. The RF transmitter and receiver would then be used to sense the cell phone reacting to the audio signal.



Magnetic Coupling Test Results

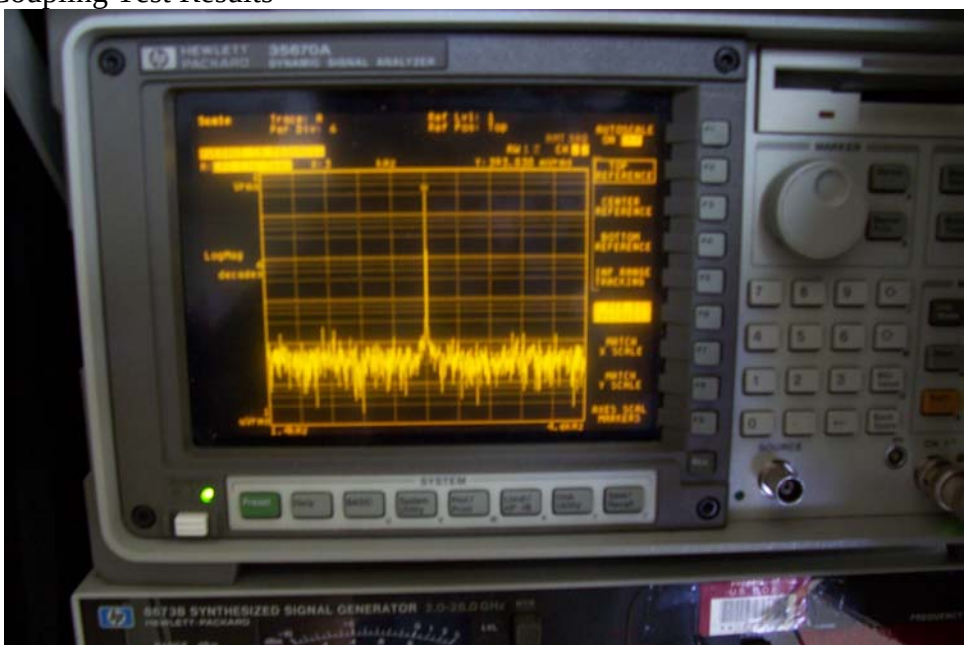


Figure 12 - Typical Magnetic Coupling and Second Harmonic Test Results

The spectrum analyzer shows a typical response from the 28MHz coils when the driven coil was modulated with 3kHz. Unfortunately, the signal amplitude did not change as a result of the cell phone being in the field.

Second Harmonic Test Results:
The typical response from this was identical to response shown in Test #1. A key observation was that the body presence could also make significant changes in the signal amplitude. Additional body distance from the antennas helped, but the presence of the cell phone did not create enough additional signal to mitigate body presence issues.

Combined Audio and RF Test results are encouraging when they occur. Power to the antenna was +30dBm (FCC specification) at 2.7GHz and the speaker was driven with $1V_{pp}$ at 2.5kHz and $55dB_{SPL}$ – normal speech is 70dB). This is not too loud to have in an access area. When no phone was present there was no signal present (see figure below). This signal is the AM demodulated fundamental frequency. I tried going higher in frequency, but that did not seem to help. The phone definitely does not respond when shielded with my hand.

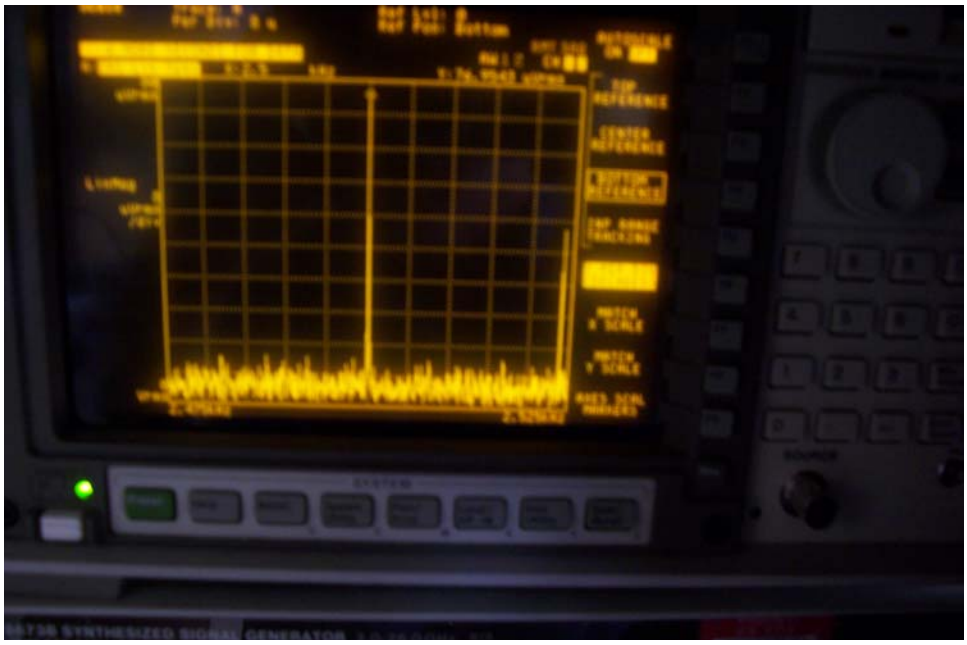


Figure 13 - Combined Audio and RF Test Results

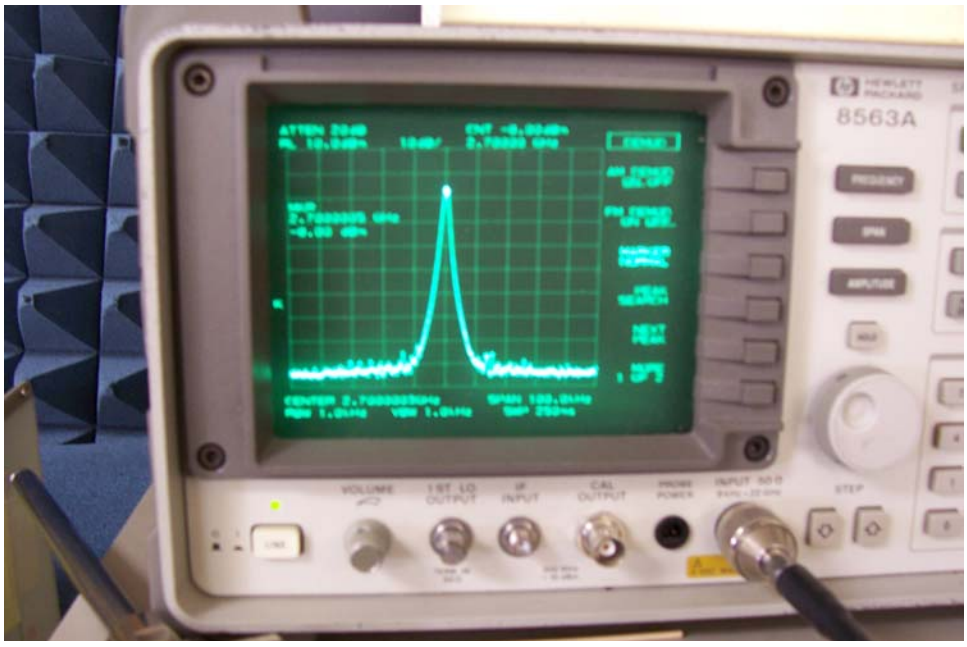


Figure 14 - Combined Audio and RF Test RF Spectrum Analyzer Signal

Seventh – Capacitive Sensor technique. A sensor similar to the one shown below was used to detect the cellular telephone. This sensor capacitively couples lower frequency energy from the phone into the sensor. This actually worked pretty well when the cellular phone was ON and within a few inches of the sensor. No external stimulus was used.

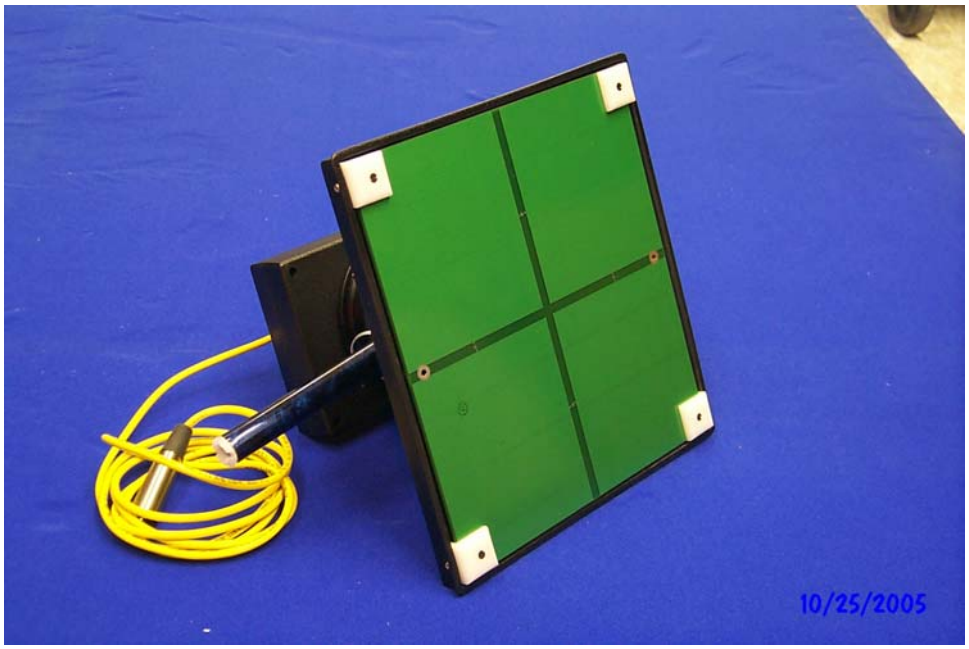


Figure 4. Capacitive Sensor

Eighth – active tags – since this is a commercial technology and has been demonstrated at Savannah River and Oak Ridge, no work has been done in this area so far. PNNL does own a Rubee evaluation kit. **RuBee** (IEEE P1902.1) is a two way radio tag protocol that uses Long Wave (LW) magnetic signals to send and receive data packets in a local regional network. The standard is in its final stages of approval by the IEEE. However the protocol has been in commercial use in asset visibility systems and networks for several years. RuBee radio tags are networked radiating transceivers, but operate at 131 kHz. IEEE P1902.1 is the physical layer workgroup and was formed in late 2006 with the final specification expected early 2008.

A typical RuBee Radio Tag - Has a 4 bit CPU, 1 Kbyte SRAM, crystal, and Li battery with expected life of five years. A typical RuBee radio tag about 1" x 1" by .070", has a 4 bit CPU, 1-5 Kbytes SRAM, a clock, optional sensors, and can have displays and buttons.

RuBee is a battery-powered, bidirectional, on-demand, peer-to-peer protocol and can operate at other frequencies. This protocol functions successfully in harsh environments with networks of many thousands of tags and has a range of 3 to 100 feet depending on the antenna configuration. By 'harsh environments' is meant the ability to read and write data near steel or water. RuBee radio tags function in environments where other radio tags and RFID may have problems.

Summary Single Method Estimated Detection Chart

Method	Range ON	Range OFF	Range Transmitting	Cost Portal	Cost Tag	Reliable Reads
Magnetic	N/A	N/A	N/A		$0	
RF Spectra	Test not Complete	Test not Complete	Test not Complete		$0	
mm-Wave	50 cm[(1)]	50 cm[(1)]	50 cm[(1)]		$0	
Phone RF	10 meters[(4)]	N/A	10 meters[(2)]		$0	
Commercial	N/A	N/A	10 meters[(3)]		$0	
RF / Audio	1 cm[(5)]	1 cm[(5)]	1 cm[(5)]		$0	
Darwin	5 cm	N/A	5 cm		$0	
Rubee Tags	1 meter[(3)]	1 meter[(3)]	1 meter[(3)]		$10	
Passive Tags	1-2 cm	1-2 cm	1-2 cm		$1	
Enhanced NLJD	50 cm	50 cm	50 cm		$1	

[(1)] All testing done at 50 centimeters. This technique is in its early R&D stages.
[(2)] Based on measured 0dBm transmitted signal level.
[(3)] Based on specification sheet.
[(4)] Technically possible to implement a "Base Station" and cause communications to initiate
[(5)] Difficult to get consistent test results using this method

Multiple Detection Method Approaches

Method 1 – Combined Passive RFID Tag and Cell Phone – This method was tested during Rubee testing at Oak Ridge / Savannah River and found to be unreliable. Measured detection range was only a few centimeters.

Method 2 – Enhanced Non-linear Junction Detector (NLJD) Method. This method added a very simple RFID tag (only a diode and the tag's antenna) to the outside of the cell phone case and detection range was evaluated. Good detection was measured out to about 50cm using test equipment with the phone ON or OFF. We will need to work through antenna / phone orientation issues.

Also considered were using magnetic or optical approach, but plausible implementations were not conceivable.

Appendix A
CellBusterSpecification

Cellbusters.Com 3240 E Hiddenview Drive, Phoenix, Arizona, 85048, USA.
Phone: 602-550-1172. Fax: 928-438-2202
email: derek.forde@cellbusters.com, web: www.cellbusters.com

Cellbuster Cell Phone Detector:

- Detect and prevent unauthorized cell phone usage.
- Automatically Alerts cell phone users to switch off their phone.
- Simple to setup, un and running in minutes.
- Range adjustment for specific area detection
- Multiple alert options
- Made in the USA, 100 % legal

The CellBuster is a device that continuously monitors for cellular phones, once it detects that a cell phone is switched on (up to 90 feet away) it will alert the phone user that they must switch off their phone.

CellBuster Features:

- Audio alert "asks" cell phone users to switch off their phone.
- Red Alert light flashes brightly to attract attention to the device if operating in audio silent mode.
- Even detects when a phone is switched on and not in use (e.g. handbag or pocket)
- Easy to configure with choice of alert modes, volume and sensitively control.
- Simple to Install no skills required - up and running in minutes.
- 100% Legal in USA, Europe and all other countries.
- Runs on four batteries which last over a year
- Saves you the embarrassment of asking someone to switch off their Cell phone.
- Remember people ignore "Cell phones are not permitted" signs

How does the CellBuster work?
The CellBuster, when turned on, will continuously monitor for radio waves emitted from wireless communication devices. The device doesn't transmit and only receives signals, therefore is safe to use in areas sensitive to Cell phones and two-way radios. The unit can even detect Cell phones hidden in handbags and briefcases.

When a signal is detected, for instance a person carrying a Cell phone in standby mode, a user selectable alarm is sounded. The unit has three alarm types.

Voice/Tone mode allows the unit to give a series of tones to alert the presence of a Cell phone, or a tone alert followed by a voice message requesting the user to stop using their communications device.

Alarm light mode flashes a bright red light, ideal for silent detection or for drawing attention to the voice message.

Remote alarm mode allows the device to send a remote signal to another device such as a security system, data logging or surveillance application.

Cellbusters.Com 3240 E Hiddenview Drive, Phoenix, Arizona, 85048, USA.
Phone: 602-550-1172. Fax: 928-438-2202
email: derek.forde@cellbusters.com, web: www.cellbusters.com

One, two, or all three alarm types can be used in conjunction with each other, ideally suiting your needs for monitoring Cell phone or two-way radio use.

Where can the CellBuster be used?
The CellBuster is ideally suited to many purposes and situations. It can be used to enforce Cell phone restricted areas such as Hospitals, Power Plants, Airports, Medical Clinics, Computer Rooms, Transportation Operations, Industrial Plants, Control Rooms, and Laboratories.

It can be used for Privacy and Security purposes where sensitive information needs to be protected, such as in Business Meetings, Financial Institutions, Courthouses, Government Buildings, Legal Briefings, Embassies, Political Meetings and Defence Facilities.

Some Examples:
Unlawful Activities can be prevented at such locations as Banks, Prisons, Security Services Firms, Detention Facilities, Police Departments, Gaming Facilities, and Facility Management Operations. By installing a Cellbuster you can monitor and protect yourself and business from unlawful use of Cell phones.

Cell phone noise pollution can be prevented in Restaurants, Bars, Privacy Rooms, Public Transport, Classrooms and Lecture Halls, Cinemas, Theatres, Golf club houses, hospitality rooms, and Church Events.

CellBuster Specifications:

- 100% Legal in USA, Europe, and all other countries.
- Informs Cell phone users to switch off their Cell phone.
- Fits anywhere, just 20Wx11.2Hx5D(cm). 8Wx4.5Hx2D(Inches).
- Built in alarm speaker.
- Weight including internal batteries is approx 2.1 lbs or 1Kg.
- Easy to wall mount or can be used as a portable device
- Battery powered (4x'C' cells) or 9v DC input jack for AC adapter (not included). Battery life is approx 1 year.
- Remote alarm output, for connection to security station or external alarm.
- Audio output for connection to external speaker.
- Integrated internal antenna, to avoid protrusions or tampering.
- Detects mobile phones and two-way radios with frequencies from 400-2000MHz
- Detects Analogue and Digital Cell phones CDMA, TDMA, GSM and PCS/PCN types.
- Sensitivity control range of 2 to 30 meters. (Approx. 6 to 90 feet).
- Low battery audio indicator.
- Easily accessible controls behind front grille, for sensitivity control, speaker volume, Alarm light (On/Off), Audio alarm type(Voice or tone), local audio alarm(On/Off), and Mobile phone Standby Mode Detection(On/Off).

Appendix B

Figure 16 (http://direct.xilinx.com/bvdocs/whitepapers/wp198.pdf) below shows a block diagram of a digital-type handset.

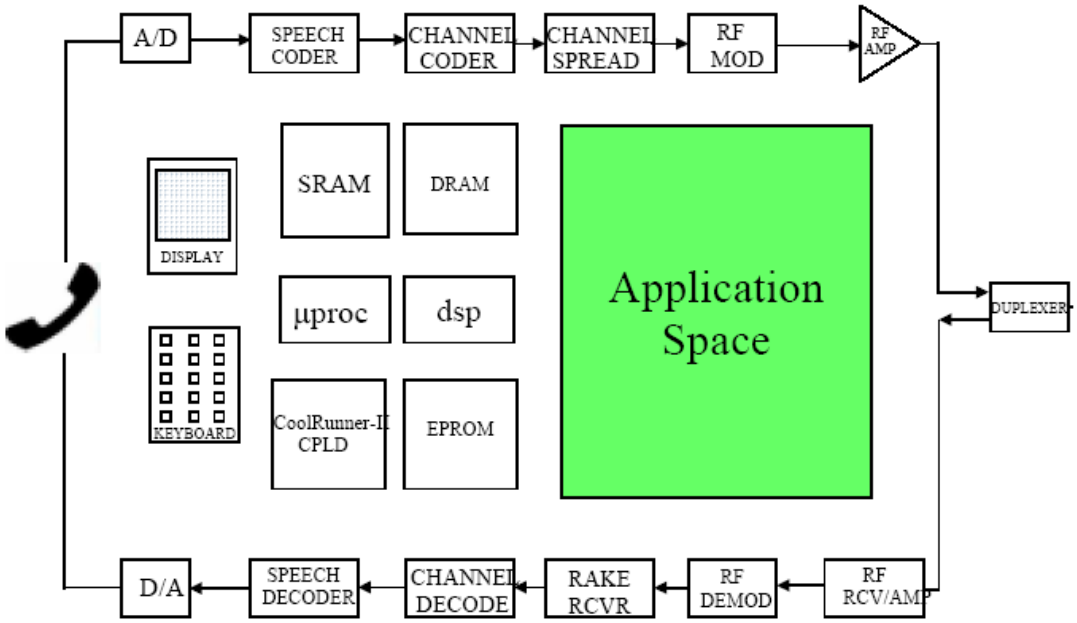


Figure 5. Functional Components of a Digital Handset / Terminal

Let's simply look at sending and receiving audio. The microphone delivers audio signal to the A/D converter, creating a bit-stream. Fidelity and efficiency require redundancy elimination and compression. This is done in the speech coder (typically adaptive multirate). Forward Error Correction (FEC) occurs in the channel coder (Viterbi today, Turbo tomorrow). Coding adds back redundancy, but dropped bits can be recovered. CDMA channel spreading has been introduced in the U.S. and Korea, but others may use TDMA, SCDMA or WCDMA. The digital signal finally gets to the RF modulator and RF amplifier where it becomes one of several signal types (again, depending on the phone standard). At this point, it is analog. Today, these are in the gigahertz range and focused on octal phase shift keying. The duplexer is inserted to switch between receiving and sending at the antenna.

On the receiving end, the signal hits the antenna, slides through the duplexer and is amplified and demodulated, becoming digital. The Rake Receiver "despreads" the received bits and forwards the signal to the channel decoder, which reconstructs the possibly corrupted digital signal and passes it on to the speech decoder. The speech decoder corrects bit-dropout and should resemble the digital version of the original analog signal. This forwards to the D/A converter, which, when filtered and amplified (not shown), drives the earphone.

But Figure 16 lacks the key items for our application – an access point into the cell phone to wake it up for reception of an incoming call. In the cases where the phone is ON, the GSM and UMTS systems use a Tree and Tabular Combined Notation to verify the protocol.

Appendix C Cellular Telephone Specifications

• ANSI/TIA/EIA-41-D, Cellular Radiotelecommunications Intersystem Operations, December, 1997.
• ANSI/TIA/EIA-93-B, Cellular Radio Telecommunications Ai - Di InterfaceStandard, December, 1997.
• TIA/EIA/IS-95-A, Mobile Station – Base Station Compatibility Standard for Dual-Mode Wideband Spread Spectrum Cellular Systems; Telecommunications Industry Association; May 1995.
• TSB74, Support for 14.4 kbps Data Rates and PCS Interaction for Wideband Spread Spectrum Cellular Systems, December, 1995.
• ANSI J-STD-008, Personal Station - Base Station Compatibility Requirements for 1.8 to 2.0 Ghz Code Division Multiple Access (CDMA) Personal Communications Systems.
• TIA/EIA-124-B, Wireless Radio Telecommunications Intersystem Non-Signaling Data Communications DMH (Data Message Handler); Telecommunications Industry Association; July 1999.
• TIA/EIA IS-136.1-A, TDMA Cellular/PCS - Radio Interface - Mobile Station —Base Station Compatibility - Digital Control Channel, Rev. A, October 1996.
• TIA/EIA IS-136.2-A, TDMA Cellular/PCS - Radio Interface - Mobile Station —Base Station Compatibility - Traffic Channels and FSK Control Channel, Rev. A, October 1996.
• EIA/TIA/IS-553, Mobile Station - Land Station Compatibility Specification; September 1989.
• TIA/EIA/IS-634, MSC - BS Interface for Public Mobile 800 MHz, December 1995.
• TIA/EIA/IS-634-A, MSC - BS Interface for Public Wireless Communications Systems, (to be published tbd).
• TSB80, MSC - BS Interface for Public 800 MHz, October 1996.
• TIA/EIA/IS-658, Data Services Interworking Function Interface for Wideband Spread Spectrum Systems, 1996.
• TIA/EIA/IS-737, IS-41-C Enhancements to Support Circuit Mode Services, (approved for publication).
• TIA/EIA/IS-683-A, Over-The-Air Service Provisioning of Mobile Stations In Spread Spectrum Systems, February 1997.
• TIA/EIA/IS-725-A, Cellular Radiotelecommunications Intersystem Operations - Over-The-Air Service Provisioning (OTASP) & Parameter Administration (OTAPA), July 1999.
• TIA/EIA/IS-756-A, TIA/EIA-41-D Enhancements for Wireless Number Portability Phase II, December 1998.
• TIA/EIA/IS-771, Wireless Intelligent Network, July 1999.
• TIA/EIA/IS-820, Removable User Identity Module (R-UIM) for TIA/EIA Spread Spectrum Standards, March 2000.
• TIA/EIA/IS-839, R-UIM Overview, Operation and File Structure Support in TIA/EIA-136-A, June 9, 2000.
• TIA/EIA/IS-841, Network Based Enhancements for User Identity Module (UIM), August, 2000.
• TIA/EIA/IS-2000, Inter-Operability Specification (IOS) for CDMA 2000 Access Network Interfaces, 2000.
• TIA/EIA/J-STD-025, Lawfully Authorized Electronic Surveillance, 2000.
• TIA/EIA/J-STD-036, Wireless Enhanced Emergency Services, 2000.