AN OPTIMAL DETECTION TECHNIQUE FOR MOBILE RADIO FREQENCIES

M.SUCHARITHA*

T.JAHNAVI*

N.POORNIMA*

P.KRISHNA SILPHA*

K MURALI**

ABSTRACT:

Cellular phone technology is rapidly changing. Features like Bluetooth, USB, high resolution cameras, microphones, Internet, 802.11 wireless, and memory cards are added every year. Also, the communication technology a cellular phone uses such as CDMA, GSM, 3G, and 4G are rapidly changing. To get a good grasp on what is available today let's take a close look at some off the shelf cellular phone detectors. Most detectors are manufactured with the intent that the cellular phone is stationary and powered on. They generally have the same features and it is questionable whether or not they actually detect a cellular phone.

The two most popular cellular phone detectors available on the market today are produced by Berkeley Varitronics Systems and Mobile Security Products. These companies produce the wolfhound cellphone detector and Cellbuster respectively. This study examines detecting cellular phones when a person is entering a secure facility or cellular phone restricted area. The detection technique studied requires measuring a cell phone's electromagnetic properties and determining an identifiable signature. Measuring the RF spectrum around 240 -400MHz(outside the cellular phone band) shows the most potential. The main problem with ensuring that a cellular phone

* VIJAYA INSTITUE OF TECHNOLOGY FOR WOMEN, Enikepadu, Vijayawada.

** Asst Professor of ECE, VIJAYA INSTITUE OF TECHNOLOGY FOR WOMEN, Enikepadu, Vijayawada.

isn't in a secure facility is that an accurate method for detecting them doesn't exist. The only way to be certain is to perform full body searches on a regular basis.

Most cellular phone detectors available today only alarm if there is a cellular phone or transmission device in the general area. They appear to alarm randomly and aren't very accurate. Detecting a cellular phone signal using an accurate signal detection technique is the focus of this research and can be solved by using a down converter in conjunction with a bandpass filter.

The technique is more accurate and provides signal detection at a lower frequency, making it easier to work with. If this solution was implemented, it would greatly reduce the risk of cellular phones getting into secure facilities. Businesses and government would save a lot of money on security. The solution would also greatly reduce the risk of their data leaking to the general public and losing even larger amounts of money.

KEYWORDS: Cellular phone detection techniques, RF spectrum, high sensitive bandpass filters, antenna radiation.

1. INTRODUCTION:

Imagine you are an IT security consultant for pharmaceutical companies. Recently a company hired you to find out why their latest drug leaked to one of their competitors prior to release. The company has many labs, each with sensitive drug information stored on computers that are closely monitored by cameras. The building they are housed in has security guards at every entrance and every employee is required to wear ID. Visitors must be escorted to ensure that no drug information leaks out. You meet with the head of security and go over the security procedures. After a little digging you find that employee-owned electronic devices such as cellular phones are allowed in and out of the facility. The company feels that the non-disclosure agreements in combination with security personnel monitoring everything on camera are strong enough to keep employees honest and that the cost of screening for electronic devices is too high. You tell the head of security that tomorrow morning security must seize every employee's electronic device as they enter the building.

The next morning you show up early and post yourself outside the entrance to the building. As people start to come into work their electronic devices are taken away. Eventually, you notice that someone walking up to the entrance immediately turns around and walks back to their car. You alert security and they find the person trying to stash away a cellular phone.

Later that morning, you download the contents of the cellular phone and find the files that were recently leaked. The employee confesses to everything and gives the details of how they did it. The files were stolen by transferring from the computers via a Bluetooth connection. Evidently, some of the computers came with Bluetooth and wasn't disabled by IT security. Using a Bluetooth connection didn't look conspicuous on camera, since there were no wires being plugged into the computer. Therefore the company needs a way to detect cellular phones in the facility. There are a few existing cellular phone detectors on the market today that could of caught the employee prior to the information leaking out. However, this technology still needs a lot of improvement and development.

2. PROBLEM FORMULATION:

In this section, we first observe the antenna radiation pattern of a cellular phone and detecting the cellular phone signal using an accurate signal detection technique can be solved by using a down converter in conjunction with a bandpass filter.

3. BACKGROUND WORK:

The two most popular cellular phone detectors available on the market today are produced by Berkeley Varitronics Systems and Mobile Security Products. These companies produce the wolfhound cell phone detector and Cellbuster respectively.

3.1 Berkeley Varitronics Systems Wolfhound Cellphone Detector

Fig 1. Wolfhound Cellphone Detector

Berkeley Varitronics Systems wolfhound cell phone detector will detect PCS, CDMA, GSM, and cellular bands using RF signatures. It also has the capability to directionally find or locate cellular phones that are nearby. The wolfhound, according to the advertisement, can detect phones that are in standby mode, actively using voice, or data transmissions.

Wolfhound cell phone detector features [2]

• 40 to 50 foot radius of coverage
• -60 dBm sensitivity
• Audible alert
• Vibrating alert
• One-handed operation
•Continually scans for cellular phone uplink activity
• Integrated laser-assisted directional antenna
• Estimated battery runtime of 18 hours

The Wolfhound on paper seems to be a great way to detect cellular phones, but may just randomly detect cellular phone communications in the area and not necessarily the phone or device that set it off. A couple of quotes from their advertisement imply this: "It took only two hours to find five cell phones that were either in use at the time or hidden in the jail cells on standby mode ready to take calls" and "With only 30 minutes of operation, the device can detect many cell phones and identify the positions which led the team to find 10 mobile phones." These two quotes suggest that their device is picking up transmissions in the area, but it doesn't show that they were directly from the phone they found or a phone at all.

Small print at the bottom of their advertisement reads, "Standby mode (autonomous registration) varies from base station to base station with phones typically registering between once every few minutes to up to 20 minutes. This time varies greatly based upon carriers, distance from base stations and individual handset manufacturer's standards ." This again casts some doubt that their equipment is easy to use and won't just be picking up random cellular transmissions or other devices in the area. Also searching the internet for reviews or feedback about the device produces no results. This uncertainty about whether the detector works makes the Wolfhound very similar to the Cellbusters cellular phone detector.

3.2 Cellbusters Cell Phone Detector

Cellbuster's cellular phone detector provides continuous monitoring for cellular phones and has a voice alert that tells the user to shut their phone off if detected. The Cellbuster only receives and doesn't transmit, making it great for areas sensitive to cellular phone usage. It will also detect phones that are in standby mode.

Cell busters cell phone detector features[1]

• Detect and prevent unauthorized cellular phone usage

• Detects analog and digital cellular phones CDMA, TDMA, GSM, and PCS/PCN types

• Range adjustment

• Audio alert asks cellular phone users to switch off their phone 10

• Red alert light flashes brightly to attract attention

• Detects when a phone is switched on and not in use

• Easy to configure and simple to install

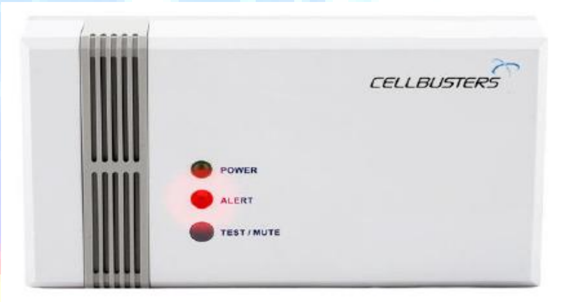

Fig 2. Cellbuster

This cellular phone detector sounds like it would work wonderfully for keeping people from bringing their phones into a secure facility. However, the advertisement isn't very honest. It doesn't tell you that a cellular phone may take up to 20 minutes to detect if it is in standby and that the phone needs to be on. Also, just like the Wolfhound, it doesn't provide any guarantee that it won't just detect random transmissions in the area.

To show how inaccurate today's cellular phone detectors are, a Cellbusters detector was borrowed from a local business and tested as part of this study. Using two LG VX11000 GSM cellular phones, this cellular phone detector was tested extensively.

4. PROPOSED WORK

4.1 Radiation Pattern of GSM

4.1.1 Power density

Power density at the antenna aperture can be approximated by the following equations:

In general:

$$S = \frac{PG}{4\pi R^2} \qquad (1)$$

Where

S = power density (in appropriate units, e.g. mW/cm2)

P = power input to the antenna (in appropriate units, e.g., mW)

G = power gain of the antenna in the direction of interest relative to an isotropic radiator

R = distance to the center of radiation of the antenna (appropriate units, e.g., cm)

In the case of aperture antennas a better theoretical estimation of the power density can be determined by using the equation showed below:

$$S_{surface} = \frac{4P}{A} \qquad (2)$$

Where

$S_{surface}$ = maximum power density at the antenna surface

P = power fed to the antenna

A = π*(D/2)^2 physical area of the aperture

4.1.2 Near field region

In the near field region of the antenna the energy is largely confined within a cylinder pattern of diameter D. The power density in that region can reach a maximum before it begins to decrease with distance and the extent of the near field can be theoretically calculated by using the following equation:

$$R_{nf} = \frac{D^2}{4\lambda} \quad (4)$$

Where

R_{nf} = extent of near-field

D = maximum dimension of antenna

(diameter if circular)

λ = wavelength

The corresponded maximum value of the power density is given by the following equation:

$$S_{nf} = \frac{16\eta P}{\pi D^2} \quad (5)$$

Where

S_{nf} = maximum near-field power density

η = aperture efficiency, typically 0.5-0.75

P = power fed to the antenna

D = antenna diameter

4.1.3 Transition region

The transition region extents from the end of the near field R_{nf} and it goes up to the beginning of the far field R_{ff} Power density in the transition region decreases inversely with distance from the antenna. To calculate the distance of the transition region we can use the following equation:

$$R_{ff} = \frac{0.6D^2}{\lambda} \quad (6)$$

where

R_{ff} = distance to beginning of far-field

D = antenna diameter

λ = wavelength

The power density can be given by the following equation:

$$S_t = \frac{S_{nf} R_{nf}}{R} \qquad (3)$$

Where

S_t = power density in the transition region

S_{nf} = maximum power density for near-field calculated above

R_{nf} = extent of near-field calculated above

R = distance to point of interest

4.1.4 Far field region

The far-field region extents for distances $R > R_{ff}$. The power density in the far-field region of the antenna pattern decreases inversely as the square of the distance. The power density in the far-field region of the radiation pattern can be estimated by the general equation discussed earlier:

$$S_{ff} = \frac{PG}{4\pi R^2} \qquad (8)$$

Where

S_{ff} = power density (on axis)

P = power fed to the antenna

G = power gain of the antenna in the direction of interest relative to an isotropic radiator

R = distance to the point of Interest

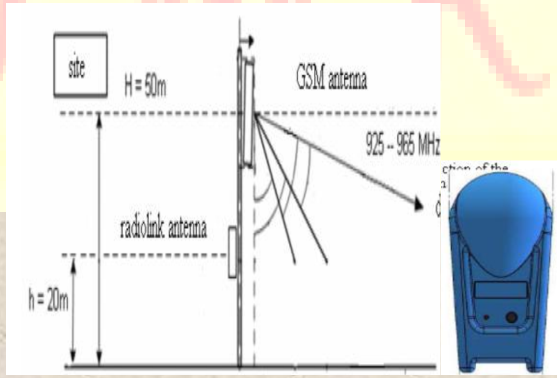

Fig 3.Graphical representation of the GSM antenna

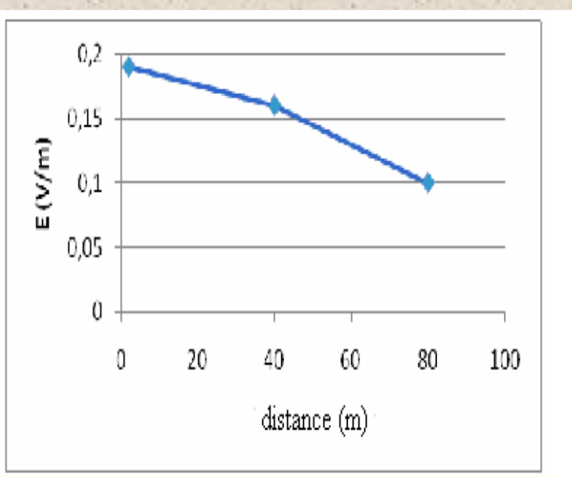

Fig 4. Electric Field strength Vs distance

4.2 High sensitive BPF:

According to previous versions, the circuit was working correctly except for the band pass filter. After studying the problem further it was determined that a computer simulation at this frequency would be less costly. Since, purchasing a band pass filter specifically made for this frequency range can cost 500 – 1000 dollars and building one with the available lab equipment would be very time consuming.

The down converter multiplies the two signals together producing the sum and the difference. This is then filtered by a band pass filter. Filtering eliminates the sum of the signals and any environmental noise. Now all that remains is the difference, a 40MHz signal that indicates an active cellular phone is in the area. This can easily converted using analog to digital converters output and output to an alarm or computer.

A simulation of the circuit in the MATLAB shows that mathematically the circuit works correctly. The following MATLAB simulation multiplies an 925 MHz sinusoid (VCO) and an 965 MHz sinusoid (input from signal generator) together. It then filters the output using a bandpass filter impulse response with a center frequency of 40MHz .The simulations in MATLAB prove that using a down converter in conjunction with a bandpass filter can accurately detect a cellular phone that is transmitting in the area. MATLAB proved that it is mathematically possible to multiplying two signals together (down converter) and filter them with a bandpass impulse response to accurately detect a signal.

5. RESULT ANALYSIS:

5.1 Radiation pattern

The Simulated results are as follows

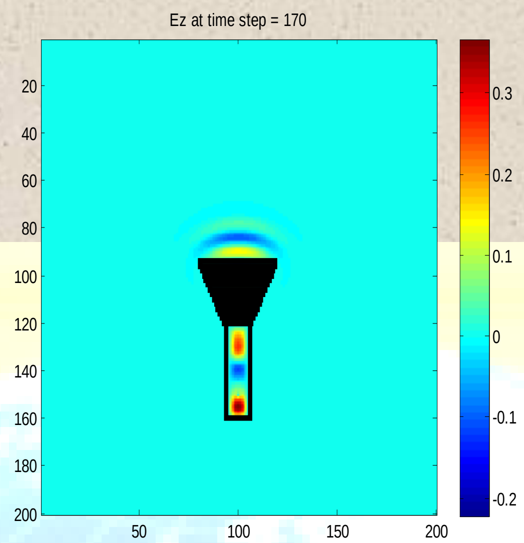

Fig 5. Radiation pattern of GSM antenna

5.2 Band Pass Filter Analysis

Figure 6 shows the impulse response of the bandpass filter that was designed in MATLAB. The filter peaks at 40 MHz and cuts all other signals down significantly as it increases or decreases in frequency.

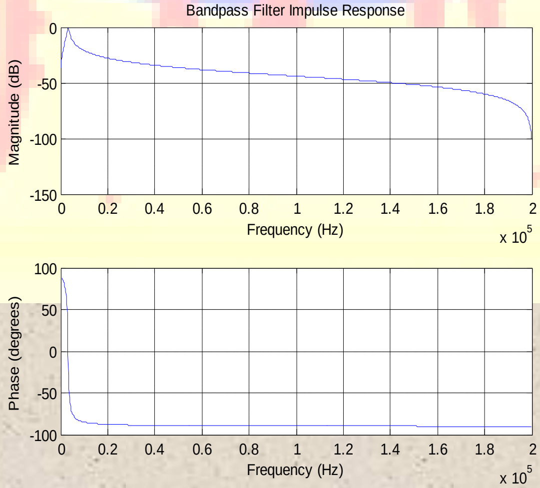

Fig 6. Bandpass Filter impulse response

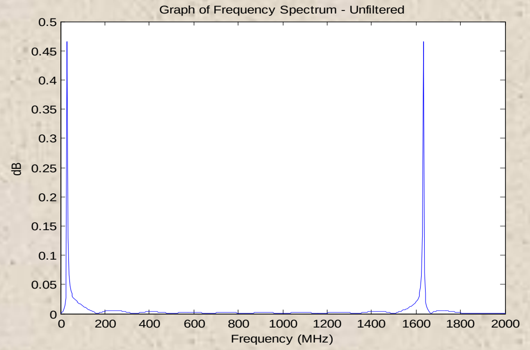

Fig 7. Unfiltered Band pass Filter Output

Figure 7 shows the frequency spectrum after the two signals have been multiplied together. This produces the sum and the difference of the signals at 1632MHz and 32MHz respectively. The output from MATLAB is very similar to the down converter used on the circuit board. Looking at Figure 3 from the output of the bandpass filter, signals in the range of the sum and difference can be seen.

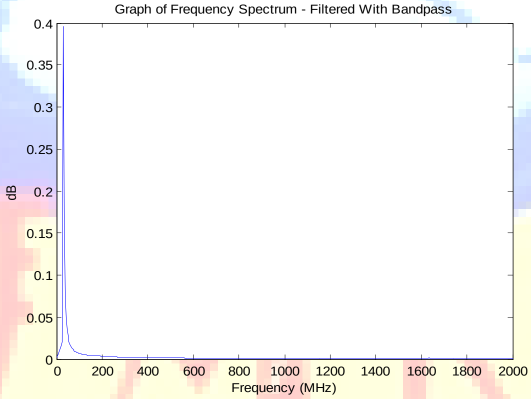

Fig 8. Output with Filtered Band pass

Figure 8 shows the output of the band pass filter. All signals except for the 32MHz signal have been cutoff. This proves that a down converter in combination with a good band pass filter will mathematically work for detecting a cellular phone.

6. CONCLUSION:

Cellular phone technology is gaining new data capabilities very rapidly. New features like Bluetooth, high resolution cameras, memory cards, and Internet make them ideal for getting data in and out of secure facilities. A cellular phone uses many different transmission protocols such as FDMA or CDMA.

Many businesses depend on keeping information protected and build fortresses that called secure facilities to protect their investment. Currently the only way to ensure that no one is bringing a cellular phone into a secure facility is to search everyone entering and exiting. This requires a lot of manpower and money to implement.

The existing technology available off the shelf does not accurately detect cellular phones in a secure facility. Detectors like the Wolfhound or Cellbusters sit in the entry way of a facility and randomly detect cellular phones or devices in the area. A better technique for accurately detecting cellular phones is needed.

This design was built and tested in the lab and proven MATLAB. Therefore computer simulation results proved that this design will work with an effective bandpass filter. This technique, if fully implemented would greatly improve cellular phone detection technology. Businesses would save money on security and save money by not allowing any sensitive information to leak out.

7. FUTURE WORK:

The hardware technique design can detect Global System for Mobile Communication (GSM) signals at 900 MHz [5].The design consists of two signal detectors each with their own dipole antenna, inductor, and diode.

8. REFERENCES:

- "CellbusterCell Phone Detector", Cellbusters INC.2004. Accessed September, 2008. Website http://www.cellbusters.com
- "Wolfhound Cellphone Detector", Berkeley Varitronics Systems. 2010. Accessed March, 2009. Website http://www.bysystems.com

- “Cell Phone Detection Techniques”, U.S. Department of Energy. October 2007. Accessed January, 2010. Website http://inspire.ornl.gov
- “Detecting and Locating Cell Phones in Correctional Facilities”, EVI Technology, LLC. June 2007. Accessed February,2010.Website http://iiw.itt.com/files/cellHound_wpCellPhonesInPrison.pdf
- “Cell Phone Detector”, Circuit-Projects.com Quality Circuits Archive.Accessed March, 2009. Website:http://www.circuit-projects.com/rf-radiofrequency- circuits/cell-phone-detector.html
- "How Cell Phones Work", How Stuff Works A Discovery Company. Accessed April, 2009. Website http://www.howstuffworks.com/cellphone.htm/printable
- Federal Communications Commission Office of Engineering & Technology: “Evaluating Compliance with FCC Guidelines for Human Exposure to Radiofrequency Fields” – OET Bulletin 65 Edition 97 – 01.
- European Union Council (1999/519/EC): “Council Recommendation of 12 July 1999 on the limitations of exposure of the general public to electromagnetic fields (0Hz to 300GHz).”
- International Commission on Non – Ionizing Radiation Protection (ICNIRP): “Guide lines for).” limiting exposure to time – varying electric, magnetic and electromagnetic fields (up to 300GHz)
- Greek Atomic Energy Commission (GAEC)