

HIDDEN ACTIVE CELL PHONE DETECTOR

¹ Anurag Saxena, ² Dr. Deepak Sharma

¹ M. Tech. Department of Electronics & Communication, Manav Bharti University, Solan (H.P), india.

² Associate Professor, RBS College, Agra, Uttar Pradesh, India

ABSTRACT

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 electronics 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 sneak 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 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 have caught the employee prior to the information leaking out. However, this technology still needs a lot of improvement and development.

INTRODUCTION:

CELLULAR PHONE TECHNOLOGY

Cellular phone technology is rapidly changing. Features like Bluetooth, USB, high resolution cameras, microphones, Internet, 802.11 wirelesses 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.

Cellular Phone Features:

Bluetooth protocol that operates at 2.4 GHz. The protocol uses a master slave structure and is very similar to having a wireless USB port on your cellular phone. Devices like a Printer, Keyboard, Mouse, Audio Device and storage device can be connected wirelessly. This feature is mainly

used for hands free devices but can also be used for file transfer of pictures, music and other data.

Universal Serial Bus(USB) is a way for cellular phones to connect to a computer for data Transfer. This feature is very similar to Bluetooth for a cellular Phone with the exception of using a cable. On today's cellular phones this features is mainly used for charging the battery or programming by the manufacturer. It can be used to transfer pictures, music and other data.

Since cameras and music have become popular features on cellular phones, manufactures have started adding memory card slots. These memory cards provide expanded memory and allow pictures to be taken or music files to be stored. Most memory cards can plug directly into the computer for easy data transfer.

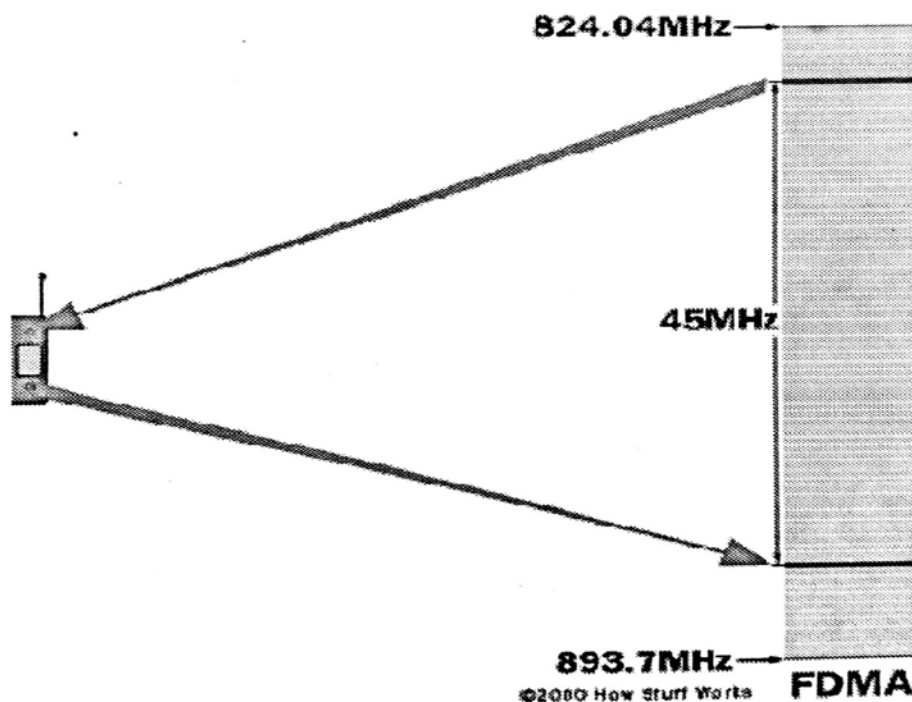


Figure 1:

Secure facilities:

Many businesses such as psychiatric hospitals, correctional facilities, pharmaceutical companies, government facilities, and many military bases rely on keeping information protected. They build security fortresses that shield their money making information from getting to the general public. These facilities have many computers that house the valuable information and are not connected to the internet. Generally, access is restricted by guards with mental detectors and electronics devices are not allowed in or out without proper approval.

In every secured facility it is hard to ensure that employees and visitors aren't violating the policies. The only way to ensure someone isn't carrying a cellular phone is to search everyone as they enter and exit. This ensures the great deal of manpower and most companies can't afford the level of security. Additionally, it will make the employees feel like the company doesn't trust them.

Cellular phone detectors available today:

To get a good grasp on what is available today let's take a close look at some off the shelf cellular phone detector. Most detectors are manufactured with the intent that the cellular phone is stationary and powered on. They

generally have the same feature and it is questionable whether not they actually detect a cellular phone.

The most important cellular phone detector available on the market today is produced by Berkeley Varitronics systems and Mobile security products. These companies produce the wolfhound cell phone detector and cell buster respectively.

Berkeley Varitronics systems wolfhound cell phone detector:

Berkeley Varitronics systems wolfhound cell phone detector will detect PCS, CDMA, GSM, and cellular bands using RF signature. 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 instruments (2).

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



Figure 2:

The wolfhound on paper seems to be a great way to detect cellular phones, but may just randomly detect cellular phone communication 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 phone that were either in use at that time or hidden in the jail cells on standby mode ready to take calls (2)" and "with only 30 minutes of operations, the device can detect many cell phones and identify the positions which led the team to find 10 mobile phones (2)". These two quotes suggest that their device is picking up transmission in that 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 with station with phones typically registering between once every few to up to 20 minutes. This time varies greatly based upon carriers, distance from base station and individual handset manufacturers standards (2)." This again casts some doubt that their equipment is easy to use and won't just be picking up random cellular transmission or other device in the area. Also searching the internet for review or feedback about the device produces so results. This uncertainty about whether the detector works makes the Wolfhound very similar to the cell buster's cellular phone detector.

CELL BUSTERS CELL PHONE DETECTOR

Cell buster's cell phone detector provides continuous monitoring for cellular phone and has a voice alert that tells the user to shut their phone off if detected. The cell buster only receives and doesn't transmit, making it great

for areas sensitivity to cellular phone usage. It will also detect phones that are in standby mode (1).

Cell buster cell phone detector features (1):

- Detect and prevent unauthorized cellular phone usage
- Detect analog and digital cellular phones CDMA, TDMA, GSM, and PCS/PCN types
- Range adjustment
- Audio alert cellular phone user to switch off their phone
- 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

This cellular phone detector sounds like it would work wonderfully for keeping people from bringing their phone 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 it guarantees that it won't just detect random transmission in the area.

To show how inaccurate today's cellular detectors are, a cell buster 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.

Following is a synopsis of the testing:

Test 1 – outside faraday cage at home with cellular phones turned on

- Tried cell detector sensitivity set low and high for 20 minutes each-detector didn't activate
- Called one phone from the other and left on for 5 minutes – detector didn't activate

- Texted one phone from the other- detector didn't activate
- Detector doesn't appear to work in public area with the sensitivity set high or low
- Detector activated randomly and generally not during a phone call

Test 2- inside faraday cage university of Nebraska Omaha with signal generator set to 832 MHz

- Tried cellular detector sensitivity set low and high for 10 minutes each- detector didn't activate
- Tried varying the frequency from 100 MHz to 1 GHz- detector didn't activate
- When set to high and open faraday cage door it would alarm sometimes testing this cellular phone detector led to a few conclusions.

The cell buster cellular phone detector doesn't work very well and it is questionable that the detector works at all. Using this device in a public area the detector just randomly went into alarm and didn't indicate where to go or what to do. Testing indicates that the cell buster's cell phone detector doesn't work as advertised.

To get an idea of the circuitry required to build a cellular phone detector, it was dismantled. Following are some pictures of the internal components.

After taking a close look at the circuitry used, no conclusion were drawn on exactly what technique of signal detection was used. Cell busters most likely used some digital signal processing to identify the signal characteristics of a cellular phone.

A study performed by the U.S department of energy out that 2 of the 5 reviewers of the product reported that it didn't work. In October 2007 when the study was performed, the cell busters cellular phone detector cost \$755 each and were backordered (3).

2.2. Related work

Since cellular phone detection is a more recent problem, there are only a few articles that have already researched this area. Two articles were published in 2007 and provide good analysis. The first, "detecting and locating cell phone in correctional facilities," was written by EVI technology, LLC. The second articles, "cell phone detection techniques" was written by a contractor hired by the U.S. department of energy (DOE).

2.2.1 Detecting and locating cell phone in correctional facilities

This article details the growing problem with cellular phones in correctional facilities and lays out the constraints used to develop their solution. According to the research, cellular phone in a correctional facility are used to operate criminal enterprises, threaten witnesses, harass victims, plan uprising, and undermine security.

Their problem is monitoring, controlling, and locating cellular phone in a correctional facility(4).

EVI's possible solution include physical search, non-linear junction detector, signal jamming, shielding, network provider location based screening, RVF detection, and their custom proprietary solution. They rule out all solution but their own custom solution that uses a system of networked sensor that are controlled by a central computer. EVI uses of proprietary software that determines the cell phones location and detects any RF emission. The location of detected cellular device is displayed on a facility map(4).

This solution was developed for detecting cellular phone in a prison. It relies on the cellular phone remaining stationary which, in prison facilities make sense since movements is limited. EVI's detection system finds cellular phone after they have already been in the facility for at least 30 minutes or if someone is making a cell phone call. EVI doesn't provide any details on the detection techniques used since it is all proprietary. Also, there are no reviews or articles stating that this system works as advised.

2.2.2 Cell phone detection techniques

This study examines detecting cellular phone when a person is entering a secure facility or cellular phone restricted area. The detection techniques studied requires measuring a cell phone's electromagnet properties and determine an identifiable signature. Measuring the RF spectrum around 240-400 MHz (outside the cellular phone band).

The DOE contractor recommends' developing a cellular phone detector by measuring the RF spectrum. Spurious emission from cellular phone are monitored and recorded when the phone is in some advantage (3):

- No external signal is required for detecting the phone
- The band of frequencies is limited by the FCC and are likely to be used by most manufactures
- System could potentially detect more than cellular phones
- This method should work on future generation of cellular phones
- System could potentially detect cellular phones even when they are off.

The authors lay out a proposed path forward for determining if this technique is possible and perform some preliminary testing of their own. They also provide an alternative path that would detect cellular phones based off of their RF reflecting material in the cellular phone filters on all phones. Cellular phones could then be detected whether are on or off (3).

This research article also mentioned an evaluation that was conducted in 2003 on the available commercial cellular phone detectors. Bechtel-Nevada and Sandia National labs found that none of the detectors at the time were effective when the phone off or in standby mode (3).

PROBLEM STATEMENT

The latest threat to information dependent businesses is the cellular phones. The technology added to cellular phones in the last 15 years has made them a jack-of-all-trades for information storage and transmission. Features like Bluetooth, USB, micro USB, high resolution cameras, microphones, internet, and 802.11 wireless make cellular phones perfect for stealing data. That is why a method to detect cellular phones in a secure facility is needed.

The main problem with ensuring that a cellular phone 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 band pass filter. The techniques are more accurate and provide 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 it 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.

PROPOSED SOLUTIONS

The first techniques explored are an existing from circuit-projects.com. This design can detect global system for mobile communication (GSM) signals at 900 MHz (5).

The design consists of two detectors each with their own dipole antenna, inductor, and diode. Each antenna is tuned to 900 MHz. when the antennas resonate at 900 MHz a charge is induced in the inductor. A diode the demodulates the signal, which is amplified by an op amp and passed along to a 3.5mm headphone jack. The design doesn't describe what sound you will hear when a cellular phone is being used, a schematic and parts list were provided.

R2, R6: 1k 1/4W Resistor

R3, R7: 8.2M 1/4W Resistor

R4, R8: 200Ohm 1/4W Resistor

R9: 2.2K 1/4W Resistor

D1, D2: BAT43 Schottky diode

C1, C2, C4: 100nf Polyester capacitor

C3: 100uf 16V Electrolytic capacitor

L1, L@: See text

U1: LM358

J1: 8 Pin socket

J2: Stereo jack

1x 9V battery

4.1.2 Block Diagram

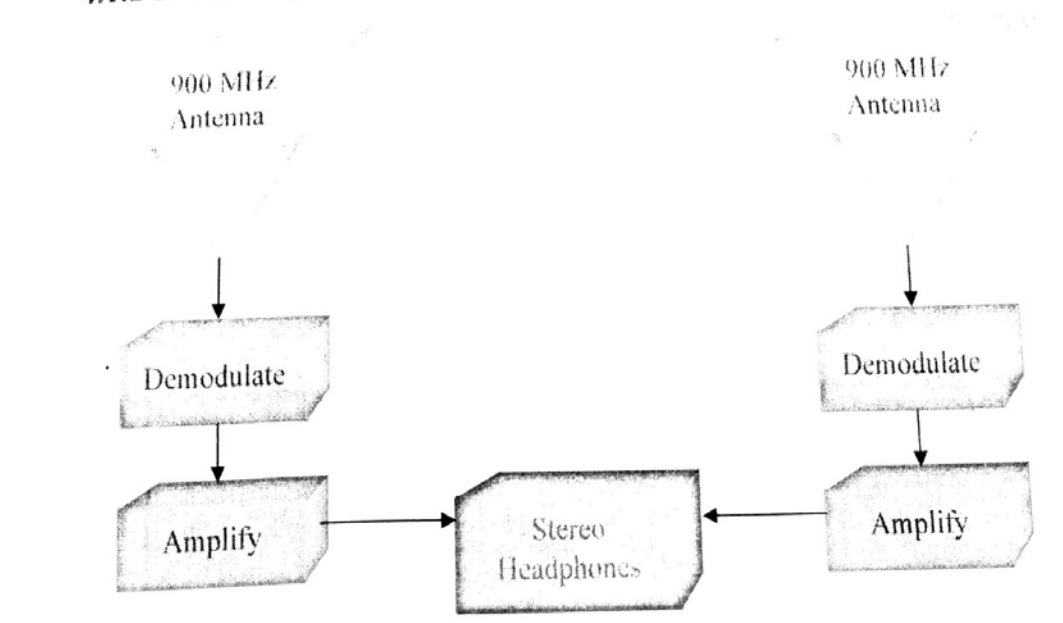


Figure 3:

4.1.3. Schematic [5]

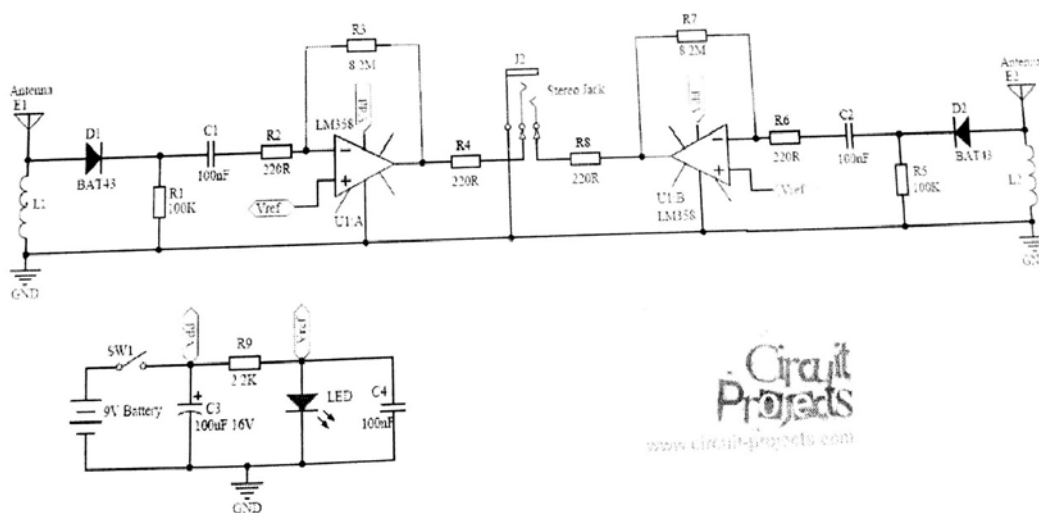


Figure 4:

RESULTS

The first test for this cellular phones detector was to just have an active cellular phone in the room. So the LG cellular phone was turned on and a phone call was placed with the detector nearby. Absolutely nothing came out of the connected head phones. To trouble shoot this problem, the circuit was tested with a spectrum analyzer and signal generator. The antenna was connected to the signal generator. The antenna was connected to the signal generator at 900 MHz with 10dB of amplitude and the spectrum analyzer was connected to the head phone jack using the antenna resulted in a lower amplitude signal on the output.

To test whether the circuit was resonating at 900 MHz, band pass test was performed by stepping the frequency at 100 MHz intervals from 600 MHz to 1.2 GHz. The amplitude changed at each intervals but was actually lower at 900 MHz than anywhere else didn't have a band pass response. The wire wrapped connections may have changed the impedance of the circuit.

While testing this cellular phone detector it was discovered that the spectrum analyzer was able to detect the LG cellular phone only using a 500 MHz probe. When taking on the cellular phones, the spectrum analyzer

spiked at 832 MHz. this gave a frequency range to design around for this cellular phone and is in the range of a GSM phone.

REFERENCES

1. Cell Buster Cell Phone Detector, Cell busters INC.2004.Accessed. September, 2008 Website: <http://www.cellbusters.com>
2. Wolfhound Cell Phone Detector, Berkeley Varitronics Systems.2010.Accessed March,2009 Website: <http://www.Bysystems.com>
3. Cell Phone Detection Techniques, U.S Department of Energy October 2007.Accessed January,2010 Website: <http://inspire.ornl.gov>
4. Detecting and Locating Cell Phones in Correctional Facilities, EVI Technology, LLC June 2007.Accessed February 2010 Website: http://iiv.itt.com/files/cellhound_wpcellphonesinprison.pdf
5. Cell Phones Detector, Circuit-Projects.com Quality Circuits Archive Accessed March 2009 Website: <http://www.circuit-projects.com/rf-radiofrequency-circuits/cell-phone-detector.html>
6. How Cell Phones Work, How Stuff Works A discovery Company Accessed April 2009 Website: <http://www.howstuffworks.cellphone.htm/printable>