The Cell Phone Detector Circuit

V Karthik Kumar[1], Kodem Sai Kumar[2], Mr. K.S.S.Naga Teja[3] and Mr. M. V. Ramani Sudha[4]

[1, 2]Final Year B.Tech, Department of Electrical and Electronics Engineering, Malla Reddy Engineering College (A), India
[3, 4]Assistant Professor, Department of Electrical and Electronics Engineering, Malla Reddy Engineering College (A). India.
E-Mail: kssnteja@gmail.com

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 electronic device as they enter the building.

Keywords – Security, Monitoring, Camera, Computer Cell Phone Detector

I. INTRODUCTION

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 2 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.

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.

Bluetooth is a secure wireless 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 3 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 feature is mainly used for charging the battery or programming by the manufacturer. It can also be used to transfer pictures, music, and other data. Cameras on cellular phones are a very popular feature that was added in the last 10 years. In recent years, high resolution cameras have become a standard feature. Most cellular phones will come with at least a 2 mega pixel camera and the more expensive phones can be as much as 8 mega pixels. Microphones have been featured on cellular phones since they first came out. In the last 10 years the microphones have become dual purpose; now there are programs on the phone that record voice to file such as a simple voice recorder or as part of a video. Almost every available cellular phone today has a connection to the Internet. This allows users to transfer files and data wherever they are. Cellular phones can send emails, text messages, picture text messages, video text messages, and upload data to the Internet. Some cellular phones come with 802.11.

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 cell phone detector and Cell buster respectively.

II. PROBLEM STATEMENT

The latest threat to information dependent businesses is the cellular phone. 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 detector 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.

III. PROPOSED SOLUTIONS

The first technique explored is an existing design from circuit-projects.com. This design can detect Global System for Mobile Communication (GSM) signals at 900 MHz. The design consists of two signal detectors each with their own dipole antenna, inductor, and diode. Each dipole antenna is tuned to 900 MHz. When the antennas resonate at 900 MHz a charge is induced in the inductor. A diode then 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.

A. Circuit Diagram Of Cell Phone Detector Circuit

The rapid growth of cell phones in the 21st century to till now has raised many problems. In addition, public reaction was growing against the disturbance of cell phones introduced in daily life. Here is a simple engineering project, namely hidden active cell phone detector. The pocket sized cell phone detector can detect the hidden active cell phone. So this project is used to neglect the use of cell phones in exam halls, private rooms, defence establishments, hospitals, military camp, petrol pumps and also very useful for sensing the use of mobile phone for spying and other correlated activities. This circuit can detect calls, SMS, video transmission even when the cell phone is hidden in silent mode. The prompt bug detects radio frequency transmission signal (RF) from a cell phone, it generates a beep sound alarm.

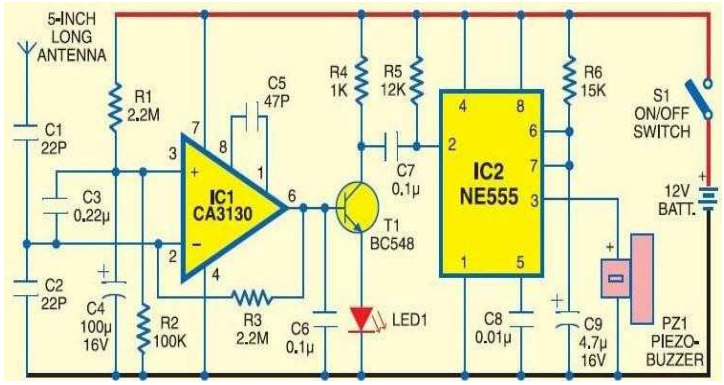

Fig. 1. Circuit of Cell phone detector circuit

The circuit of cell phone detector is shown in the above Fig. 1. The transmission frequency of cell phones ranges from 0.9Hz -3GHz with a 3.3cm - 10cm wavelength. RF signals can be collected from the cell phone along with the disk capacitor and the leads which acts as a small gigahertz loop antenna. When the cell phone is triggered, it transfers the signal in sine wave form which permits through the space. The circuit diagram of the hidden active cell phone detector is built with operational amplifier, monostable multi vibrator and piezo buzzer. An ordinary RF detector using tuned LC circuits is not suitable for detecting signals in the GHz frequency band used in mobile phones. The transmission frequency of mobile phones ranges from 0.9 to 3 GHz with a wavelength of 3.3 to 10 cm. So a circuit detecting gigahertz signals is required for a cell phone detector. Here the circuit uses a 0.22pF disk capacitor (C3) to capture the RF signals from the mobile phone. The lead length of the capacitor is fixed as 18 mm with a spacing of 8 mm between the leads to get the desired frequency. The disk capacitor along with the leads acts as a small gigahertz loop antenna to collect the RF signals from the mobile phone.

IV. Working And Operation Of Cellphone Detector Circuit

The main concept of this project is to detect the existence of an activated cell phone from a distance of one and a half meters to avoid the use of cell phones in the hospitals, examination halls, etc. This proposed system is very helpful in particular places like exam halls, offices, temples and theatres where uses of cell phones are not permitted to sense and control the use of cell phones. This project is used to detect the active cell phone, when somebody is trying to make or receive a call, sending or receiving a message. A buzzer gives an alert in the occurrence of an active mobile phone in the distance of one and a half meters in the above mentioned conditions.

A. Principle Of Cellphone Detection

When mobile phone is active, it transmits the signal in the form of sine wave which passes through the space. The encoded audio/video signal contains electromagnetic radiation which is picked up by the receiver in the base station. The transmitter power of the modern 2G antenna in the base station is 20-100 watts. The mobile phone transmits short signals at regular intervals to register its availability to the nearest base station. Distance to cellular base station is the most important environmental factor. Generally, the nearer a cellular phone is to a base station or transmitting tower, the weaker will be the signal that needs to come from the phone. Range of frequencies of different categories are, AM radio frequencies between 180 kHz and 1.6MHz,FM radio uses 88 to 180 MHz, TV uses 470 to 854MHz.waves at higher frequencies but within the RF region is called Micro waves. Mobile phone uses high frequency RF wave in the micro wave region carrying huge amount of electromagnetic energy.

B. Working Of Cell Phone Detector Circuit

This handy mobile bug or cell phone detector, pocket-size mobile transmission detector or sniffer can sense the presence of an activated mobile cellphone from a distance of one and-a-half metres. So it can be used to prevent use of mobile phones in examination halls, confidential rooms, etc. It is also useful for detecting the use of mobile phone for spying and unauthorized video transmission. In the proposed system, an RF signal detector using tuned LC circuits is designed for detecting signals in the GHz frequency band used in mobile phones as the transmission frequency of mobile phone ranges from 0.9 to 3 GHz. A capacitor C and L are used to form the LC circuit to receive radio frequency signals from the cell phone. When the cell phone is triggered the radio frequency transmission signal is sensed by the detector and generates a beep sound and the LED will glow. The transmission frequency of mobile phones ranges from 0.9 to 3 GHz with a wavelength of 3.3 to 10 cm. So a circuit detecting gigahertz signals is required for a mobile bug. The lead length of the capacitor is fixed as 18 mm with a spacing of 8 mm between the leads to get the desired frequency. The disk capacitor along with the leads acts as a small gigahertz loop antenna to collect the RF signals from the mobile phone.

V. Result

The prototype version has only limited range of less than 1 metre. In this project we made an attempt to design a mobile detector which can detect both the incoming and outgoing calls as well as video transmission even if the mobile is kept at the silent mode. The below shown in Fig 7.1 is the cell phone detector circuit made by us.

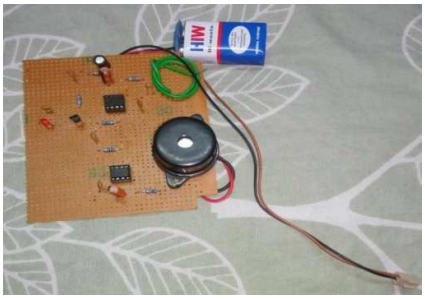

Fig. 2. The Cell Phone Detector Circuit

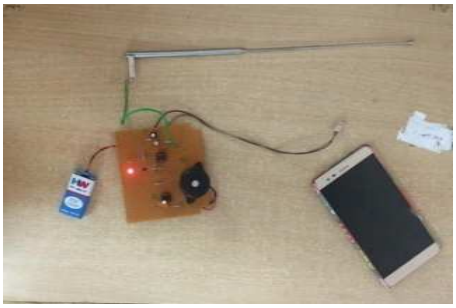

Fig. 3. Cell phone detector circuit in working condition

Our circuit has detected the presence of an active mobile phone at a distance of less than one meter. It gave the indication of an active mobile phone by glowing the LED, according to the receiving frequency and by buzzing the sound of the buzzer. The alarm continues until the signal is ceases. Here we would also like to add that it is just a prototype of our project and can be less used for Real time operations as the range of detection is not too great which can be advantageous at few situations. Below is the figure Fig showing that the circuit is in working condition.

VI. Conclusion

This pocket-size mobile transmission detector or sniffer can sense the presence of an activated mobile cell phone from a distance less than one and-a-half meters. So it can be used to prevent use of mobile phones in examination halls, confidential rooms, etc. It is also useful for detecting the use of mobile phone for spying and unauthorised video transmission. In this project we made an attempt to design a mobile detector which can detect both the incoming and

outgoing calls as well as video transmission even if the mobile is kept at the silent mode. Our circuit has detected the presence of an active mobile phone even at a distance of about one and half a meter. It gave the indication of an active mobile phone by glowing the LED, according to the receiving frequency and by buzzing the sound of the buzzer. The alarm continues until the signal is ceases

VII. FUTURE SCOPE

Trying to increase the detecting range of mobile bug to few more meters for observing wide ranges of area. In the future time this detector will be improved in all ways. In future we could be able to detect any range of frequency over a meters of range and this will be very useful to detect the cell phones where the cell phones are prohibited.

REFERENCES

[1] Cell buster Cell Phone Detector", Cell busters INC.2004. Accessed September, 2008. Website http://www.cellbusters.com.
[2]]"Cell Phone Detection Techniques", U.S. Department of Energy. October 2007. Accessed January, 2010. Website http://inspire.ornl.gov.
[3] A.V.Sudhakara Reddy, M. Ramasekhara Reddy, M. Vijaya Kumar "Stability Improvement During Damping of Low Frequency Oscillations with Fuzzy Logic Controller", International Journal of Engineering Research and Applications (IJERA), Vol.2, No.5, pp.1560-1565, September 2012.
[4] P Prasad, B Bhargava Reddy and A V Sudhakara Reddy "Power Loss Minimization in Distribution System using Network Reconfiguration with Particle Swarm Optimization", International Journal of Engineering Science & Advanced Technology, Vol.5, Iss.3, pp.171-178, May 2015.
[5] K.Surekha and A.V.Sudhakara Reddy "A New Control Topology for Smart Power Grids using Bi-directional Synchronous VSC", International Journal of Informative & FuturisticResearch, Vol.2, No.10, PP.3695-3704, June 2015.
[6] B Bhargava Reddy, D Sivakrishna and A V Sudhakara Reddy "Modelling and Analysis of Wind Power Generation Using PID Controller", International Journal For Scientific Research & Development (IJSRD), Vol.1, No.9, pp.2045-2049, November 2013.
[7] A. V. Sudhakara Reddy, Prof. M. Damodar Reddy, "Optimization of network reconfiguration by using particle swarm optimization",2016 IEEE First International Conference on Power Electronics, Intelligent Control and Energy Systems (ICPEICES-2016), July 4th - 6th, 2016.
[8] S.Bharathi, A.V.Sudhakara Reddy and M.Damodar Reddy, "Optimal Placement of UPFC and SVC using Moth-Flame Optimization Algorithm", International Journal of Soft Computing and Artificial Intelligence, ISSN: 2321-4046, Vol.5, No.1, pp.41-45, May2017.
[9] A. V. Sudhakara Reddy, M. Damodar Reddy and N.Vinoda, "Optimal Placement of Dynamic Voltage Restorer in Distribution Systems for Voltage Improvement Using Particle Swarm Optimization", International Journal of Engineering Research and Applications (IJERA), ISSN: 2248-9622, Vol.7, No.3, pp.29-33, March 2017.