Design and Testing of Mobile-Phone-Detectors

Edwin Ataro* Diana Starovoytova Madara Simiuy Sitati School of Engineering, Moi University P. O. Box 3900, Eldoret, Kenya

Abstract

Students use mobile-phones to store lecture-materials, e-books, tutorials, videos, communicate with their classmates and browse the internet for exceedingly-different-intentions. These projected-advantages, however, would have potential-undesirable-effects if mobile-phones are utilized in restricted-premises, such as exam-venues. Noncompliant- students (to general University exam-regulations) do use mobile-phones to cheat in exams. The rapid-explosion of cell-phones at the beginning of the 21st Century eventually raised problems, such as their potential-use to invade privacy or contribute to widespread academic-cheating. In this paper, two systems, that will be used, independently, to detect mobile-phones in the exam-venues, were proposed: a mobile-detector with a range of 1.0m, using resistor-capacitor-circuit, which can detect both the incoming and outgoing-calls, as well as video-transmission and text messages, even if a mobile-phone is kept at the silent mode; and a Reed-switch-circuit-scanner, which, responds to an applied-magnetic-field and, can be used to detect mobile-phones that are switched-off or put on flight-mode, and thus, it can be used to scan students (without physical-inspection) on their entering examination-rooms. Overall, the results of this-concise-study are rather-positive, providing a good-starting-point for advanced investigations and improvements of the same. Several future-research-areas were also proposed by the study.

Keywords: mobile, phone, students, detector, cheating.

1. Introduction

1.1. ICTs progression

Information and communication technologies (ICTs) are a diverse set of technological tools and resources, used to communicate, and to create, disseminate, store and manage information (Blurton, 2002). They include computers, internet, broadcasting technologies (radio and television) and telephony (mobile-technology). ICTs are powerful-tools that can increase access to improved and quality-education. For most students, the advent of mobile-phones, hand-held devices including, digital-readers and the internet, has greatly enhanced interpersonal-communication and education. Hand-held-devices have enabled users to access and retain great amounts of information for future references. Indeed, the emergence of these technological-tools has significantly improved education, research and school-work.

The advancement and wide-usage of mobile-phones have promoted them to become the learning- media, increasing integration of mobile-phones into instruction in the Universities (Masri, 2015). In spite of the vital-role that is played by mobile-phones as a learning-tool, there still are challenges that could originate from using mobile-phones, such as cheating during exams and distraction during lecture-hours. Nyamawe & Mtonyole (2014), for example, observed that, recently university-authorities have noted an overwhelming-increase in the use of mobile-phones by students to cheat during examination.

1.2 Mobile/Cellular- phone operation and capabilities

A mobile-phone (also known as a cellular-phone, cell-phone, a mobile, and a hand-phone) is a device that can make and receive phone-calls over a radio-link, while moving around a wide-geographic-area. It has made it possible for a person located in a remote-place to communicate with a person across the globe in a fraction of a second. It does so by connecting to a cellular-network provided by a mobile-phone-operator, allowing access to a public-telephone- network.

Mobile-phone uses RF ranging from 700 to 2600 MHz in the GSM (Global-System of Mobile communication) and LTE (Long Term Evolution) bands, that is the signal is high-frequency with huge-energy (Shon, 2006). When a mobile-phone is active, it transmits the signal in the form of sinusoidal-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. Mobile-phone system is referred to as "Cellular-Telephone-system" because the coverage-area is divided into "cells", each of which has a base-station. The transmitter-power of the modern 2G antenna in the base-station is 20-100 Watts (Sujith, 2014).

When a GSM digital-phone is transmitting, the signal is time-shared with 7 other users. That is in any one second, each of the 8 users on the same-frequency is allotted 1/8 of the time and the signal is reconstituted by the receiver to form the speech. Peak-power-output of a mobile-phone corresponds to 2 Watts with an average of 250 milli-Watts of continuous-power. Each hand-set within a 'cell' is allotted a particular-frequency for its use. The mobile-phone transmits short-signals at regular-intervals to register its availability to the nearest- base-station. The network data-base stores the information transmitted by the mobile-phone. If the mobile-phone moves from

one cell to another, it will keep the connection with the base-station having the strongest-transmission. A mobilephone always tries to make connection with the available base-station. AM Radio uses frequencies between 180 kHz and 1.6 MHz, FM radio uses 88 to 180 MHz, TV uses 470 to 854 MHz-waves at higher-frequencies, but within the RF-region is called micro-waves. The strongest-radiation from the mobile-phone is about 2 Watts, which can make connection with a base-station located 2 to 3 km away (Shon, 2006).

Modern mobile-phones support a wide-variety of other services such as text-messaging, MMS, email, internet-access, short-range 802.11 wireless communications (infrared, Bluetooth), business-applications, gaming, high-resolution-video-cameras enabling video and photography; microphones allowing to record telephone-conversations and other audio-signals. Mobile-phones also allow running of small computer programs (mobile apps), which provide a variety of features including: viewing and editing of text-files in different-formats such as word, ppt and pdf, instant-chatting, web-browsers, dictionaries, and scientific-calculators among others. Today's mobile-phones have increasingly become hi-tech; mobile-phones have storage-capacity, Random Access Memory (RAM), Internal-memory, and Extended memory as memory-cards, Processing-power (CPU), Built-in sensors, GPS, USB, and operating systems, just to cite a few. Mobile-phones that offer these and more-general computing-capabilities are referred to as smart-phones. Furthermore, the communication-technology a cellular-phone uses such as CDMA, GSM, 3G and 4G is rapidly-modernizing (Okebukola, 2014).

With all these impressive-advantages, that mobile-phones could offer, there are still many-premises in which the use of mobile-phones should be strictly-prohibited. Therefore, the growing use of cell-phones has somewhat made it mandatory to find ways to detect and prevent its usage in restricted or high-security areas.

1.3. Cheating in examinations with a mobile-phone and its consequences

Cheating with technology include (but not limited to) the use of cell-phones, programmable-calculators, pagers, personal-digital-assistants (PDAs), computers, internet and so on to gain unfair-advantage in examinations. The motive behind taking mobile-phones in the examination-room by the desperate-candidates is to illegally get access to answers, which is considered as cheating. Most Universities, including the Moi University of Kenya, have explicit exams-regulations stating, that mobile-phones are strictly-prohibited in the examination-rooms.

The capability of today's mobile phones gives a student numerous ways to cheat in exams. During exams period, a student may constantly-communicate with people outside the exam-room via email and use Short Messaging Services (sms). Students and outsiders can exchange information (Questions and Answers) via email-attachments. Through a mobile-phone-camera, a student can snapshot questions and sends as an email or WhatsApp attachment to outsiders for help, and in the same-way a student can receive answers. Moreover, as mobile-phone provides internet- connectivity, student can post questions online and receive responses instantly. In addition to that, a student can post their inquiries to search engines and look for answers from many engines. Furthermore, with the storage-capacity that mobile-phone offers, students can pack lecture-notes, e-books and any other unauthorized-materials relevant to the exam in question on their mobile-phones, sometimes before examperiod. Other applications installed in a mobile-phone could also be used by a student to commit cheating; such applications include dictionaries and scientific-calculators. As technology keeps advancing, likewise the students get access to multiple-technologies to commit academically dishonest-acts of cheating (Styron & Ronald, 2010).

Cheating creates unfair competition amongst students in a class (Yee & MacKown, 2014). The implications of examination-malpractice among students are frightening and devastating. Examination-malpractice destroys the foundation and fabric of any educational-system. It makes formal-assessments unreliable, educational-objectives unattainable and portends a bleak-future for any-society. The emergence of e-cheating has added to the challenges of conducting credible and reliable-examinations (Alonge, 2003).

Cheating in exams is a serious problem that has negative-educational, social and psychological effects. Educationally, cheating is contrary to the spirit of education, especially in building and promoting high-moralvalues and attitudes. Moreover, it violates institutional regulations, and it is an indicator of an educationalinstitution inability to provide an educational-process that offers equal-opportunities for all students to learn. In addition, cheating negatively-affects the accuracy of the evaluation-process by adding more sources of errors, which decreases exams-validity and reliability. Socially, cheating is unacceptable- behavior to get something one is not entitled to. Cheating not only affects students who cheated, but also affects other-students, as it forces them to live in an unfair-system. Perhaps, most importantly, cheating-behavior may carry-over after graduation. Psychologically, cheating may compromise a student's values, potentially resulting in serious-psychologicalproblems, such as feelings of guilt and shame. This, in turn, would have negative-effects on a student's self-respect, self-esteem, level of motivation, and learning- ability (Bruno & Igbo, 2012).

It is therefore important to always reflect and develop new-ways of combating emerging-technologies that could potentially be used for cheating in exams.

1.4. Statement of the problem and purpose of the study

The rapid-explosion of cell-phones at the beginning of the 21st Century eventually raised problems such as their

potential-use to invade privacy or contribute to rampant academic-cheating. Curran *et al.* (2011), suggested that, it is evident that counter-measures are needed so as to fight against cheating with technology, which is continuously growing. One of the existing-approaches to ensure students are free of mobile-phones in exam-venues is through manual/physical-inspection during exam-venue-entrance, which viewed by some students and lecturers as invasive and sometimes even in-effective. Manual-inspection cannot reveal 100% the presence of mobile-phones and therefore some students may go undetected, especially if they hide a mobile-phone in their private-parts. In some instances, for example, students can even manage to bring 2 mobile-phones, knowing that they will have to surrender one before the exam, so that they can use the second-phone during the examination. Taking into consideration that, some unauthorized-users of mobile-phones may not be uncovered by invigilators during examination, better-techniques for detecting unauthorized-usage of mobile-phones during examination-time is needed (Lawal *et al*, 2013). With the help of cell-phone-detectors the examiner will know if a cell-phone is active and can take appropriate-action immediately.

In recent years, there has been also an increasing-focus on issues relating to the use of mobile-phones in restricted, prohibited, and unauthorized-areas. The reason for this increased-interest is largely due to disturbance, as well as wrong and inappropriate-usage of mobile-phones by the owners and users alike. Areas like banks, courts of law, churches/mosques/synagogues, offices, private meeting-venues, restaurants/hotels, prisons, airports, theatres/cinemas, conference-facilities, museums, hospitals, examination-halls, defense and security-establishments, military and police-base-camps, hospitals; and petrol-stations and depots among others, just to mention a few, are where the use of an active Mobile Communication (GSM) device are prohibited/limited. However, with all the potential-benefits that are offered by today's mobile-phones, researches, designers and government-leaders are still pondering the provisioning of mobile-phones-detectors in all the restricted-areas. To avoid an unauthorized-use of mobile-phones in all restricted areas, the use of mobile-phones-detectors is therefore necessary and timely.

This study, therefore, proposes simple mobile-phone-detection systems. The purpose of the study is to: Design, fabricate and validate/test two detection-systems; and do a financial-evaluation of the systems. Although this design is particularly focused on preventing cheating in examinations, this work is also potentially-useful not only for mobile-phone detection during examinations, but also for other unauthorized-usage of mobile- phones in restricted/sensitive areas with limited/prohibited mobile- phone-assess.

2. Materials and methods

2.1. Materials

The following materials were used in this study:

Mobile Phone: A wireless communication device through which the RF-signals are transmitted or received and whose presence is to be detected by the mobile-phone-detectors. Smartphone Samsung Galaxy Ace S5830 powered by Android 2.2 OS platform was used an as major test-tool of this-study. Android is a Linux-based operating-system designed primarily for touch-screen-mobile-devices such as Smart-phones and tablet-computers.

Antenna: The antenna is used to sense the RF-signals that is being transmitted or received through the mobile- phones. Here the length of the antenna is 5-inches (around 13 cm).

Operational Amplifier (Op-Amp)-A direct-current coupled high gain electronic-voltage-amplifier with a differential- input and usually a single-ended-output. The Op-amp used in the circuit functions as a current to voltage converter. The Op-amp output becomes high and low alternately according to the frequency of the signal detected from the mobile-phones.

Integrated Circuit-Lm 358p – is a set of electronic-circuits. The LM358 IC is a great, low-power and easy to use dual-channel op-amp IC. It consists of two internally-frequency-compensated, high-gain, and independent op-amps. This IC is designed specially to operate from a single-power-supply over a wide range of voltages. The LM358 IC is available in a chip-sized-package and applications of this op-amp include conventional op-amp circuits, DC- gain-blocks and transducer-amplifiers. It can handle 3-32V DC supply and source up to 20mA per channel. This op-amp is apt, if you want to operate two separate op-amps on a single-power-supply.

Mono-stable-Multi-vibrator: The output of Op-Amp triggers the Mono-stable- Multi-vibrator circuit and produces pulse waveforms as the output.

Piezo-Buzzer: A buzzer or beeper is a signalling device, usually electronic, typically used in automobiles, household appliances such as micro-wave-ovens. It most-commonly consists of a number of switches or sensors connected to a control-unit that determines if and which button was pushed or a pre-set-time has lapsed, and usually illuminates a light on the appropriate-button or control-panel, and sounds a warning in the form of a continuous or intermittent- buzzing or beeping-sound. The piezo-buzzer usually produces sound when the output of the RF-detector goes high.

Reed Switch: is actuated by magnets, and commonly used in mechanical-systems as proximity-sensors. Examples are door and window-sensors in burglar-alarm-systems and tamper-proofing-methods (however they

can be disabled by a strong, external-magnetic-field). Reed-switches are used in modern-laptops to put the laptop on sleep/hibernation-mode when the lid is closed. The reed-switch is an electrical-switch operated by an applied magnetic-field. A magnetic-field (from an electromagnet or a permanent magnet) will cause the reeds to come together, thus completing an electrical circuit. The stiffness of the reeds causes them to separate, and open the circuit, when the magnetic field ceases. Good-electrical-contact is assured by plating a thin layer of non-ferrous precious-metal over the flat-contact-portions of the reeds. Since the contacts of the reed-switch are sealed away from the atmosphere, they are protected against atmospheric-corrosion. The hermetic-sealing of a reed-switch make them suitable for use in explosive-atmospheres where tiny sparks from conventional switches would constitute a hazard.

Reed Relay- One or more reed-switches inside a coil is a reed-relay. Reed-relays are used when operatingcurrents are relatively-low, and offer high-operating-speed, good-performance with very-small-currents which are not reliably switched by conventional-contacts.

Battery VVC 9V- The nine-volt battery, or 9-volt battery, in its most-common-form was introduced for the early transistor-radios. It has a rectangular-prism-shape with rounded-edges and a polarized-snap-connector at the top.

LED -a light-emitting diode is an electronic-light-source. LEDs are used as indicator-lamps in many kinds of electronics and increasingly for lighting. LEDs work by the effect of electroluminescence, discovered by accident in 1907. LEDs are based on the semiconductor-diode. When the diode is forward-biased (switched-on), electrons are able to recombine with holes and energy is released in the form of light. This effect is called electroluminescence and the color of the light is determined by the energy-gap of the semiconductor.

Resistors- A resistor is a two-terminal electronic-component that produces a voltage across its terminals that is proportional to the electric-current through it. Resistors are elements of electrical-networks and electronic-circuits and are ubiquitous in most electronic-equipment. Practical-resistors can be made of various-compounds and films, as well as resistance-wire (wire made of a high-resistivity-alloy, such as nickel/chrome). The primary-characteristics of a resistor are the resistance, the tolerance, maximum working voltage and the power-rating.

A capacitor or condenser- is a passive-electronic-component consisting of a pair of conductors separated by a dielectric. When a voltage-potential-difference exists between the conductors, an electric-field is present in the dielectric. This field stores energy and produces a mechanical-force between the plates. Capacitors are widely used in electronic-circuits to block the flow of direct-current while allowing alternating-current to pass, to filter out interference, to smooth the output of power supplies, and for many other purposes.

2.2 Methods

The design-approach of 2 detectors is shown in Figure 1.

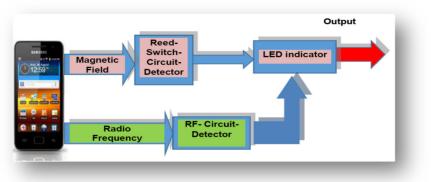


Figure 1: Design-approach of two-detectors

The transmission-frequency of mobile-phones ranges from 0.9 to 3 GHz with a wavelength of 3.3 to 10 cm. Therefore a circuit detecting gigahertz-signals is required for a mobile-phone-detector.

Circuits were designed and first tested on a breadboard; then the circuits were assembled on a generalpurpose PCB as compact as possible and enclosed in a small box, looking like an old-primitive mobile-phone (to camouflage the detector).

A printed circuit board (PCB) is a self-contained-module of interconnected-electronic-component found in devices from common-beepers, or pagers, and radios to sophisticated-radar and computer-systems. The circuit is formed by a thin layer of conducting material deposited or printed on the surface of an insulating board known as the substrate. Individual-electronic-components are placed on the surface of the substrate and soldered to the interconnecting-circuit. After the print-out, the design on this special paper is then ironed onto the board (substrate), which leaves the circuit-path on the board. The substrate is then etched leaving only the conducting-circuit-path on the board, after this, the electronic-components are drilled and the whole-board is cleaned and ready for the components to be placed into position.

3. Results and discussions

3. 1. Review of literature on previous works

The review recorded below does not claim to be a fully-comprehensive-account of every-instance related to mobile-phone-detectors, but it does give a fairly-good-picture of the status of activities, achievements, and problems encountered, and probably include the most-significant-ones-identified for which information was available at the time this study was carried out.

The first-signal-detection-technique, an RF-detector using tuned-Inductor-Capacitor (LC) utilizes discrete- components which is difficult to implement (Ajasa, et. al., 2014). It is very-affordable to construct, but requires precision- tuning. This design when analyzed was also found to be inaccurate.

The second-technique seems to be accurate, but has its own- short-comings, in addition to being very expensive. The two-most-popular mobile-phone-detectors available under this technology are produced by Berkeley Varitronics Systems and Mobile Security products. These companies produce the Wolfhound cell-phone-detector and cell-buster, respectively. The Berkeley Varitronics systems Wolfhound cell-phone detects Personal Computers (PCs), Code Division Multiple Access (CDMA), Global System for Mobiles (GSM) and cellular-bands using the RF-signals. It is also capable to directionally find and locate cellular-phones that are nearby (Wolfhound Cell-phone-Detector, 2013).

The Wolfhound seems to be a great-way to detect cellular-phones but may just randomly detect mobilephone-communications in the area and not necessarily the Phone or device that set it off. The Cell-Buster from Mobile Security Product provides continuous-monitoring for mobile-phone and has voice-alert that tells the user to shut their-phone-off if detected. The Cell-Buster only receives and does not transmit, making it great for areas that are sensitive to cellular-phone-usage. It also detects phones that are in standby mode. The Cell-Buster also seems like it would work wonderfully for keeping people from bringing their phones into restricted areas, however, like the Berkeley Vantronics systems it has its shortcomings as it takes up to 20 minutes to detect if it on standby and that the phone needs to be on and its detection could be random transmission in that area.

Efforts have been put in place in tackling the issue of cheating in examinations, but they all have theirown- shortcomings, one of which is the mobile-phone-jammer. A mobile-phone-jammer is an instrument used to prevent cellular-phones from receiving signals from base-stations. When used, the jammer effectively disables cellular-phones. These devices can be used in practically any location, but are found primarily in places where a phone call would be particularly disruptive because silence is expected (Blog-jammer-store, 2009). The shortcoming of such a technology is the complete inability to make calls, especially in cases of emergencies.

A novel mobile-detector-sensing alarming and reporting system developed by Mohan (2012) had a pivotal role to detect mobile-phones in restricted-areas. Through an antenna, the device detects the presence of a mobile-phone and a signal is sent to PIC16F877A microcontroller which turns ON the buzzer-circuit and sends the message to an LCD-module for display and as well an SMS is sent to the registered mobile-number via GSM module for notification.

An intelligent-mobile-phone-detector designed by Mbaocha (2012), was able to detect the presence of GSM-signals emitted from a mobile-phone within the radius of 1.5 meters. A device had a capability to detect calls, SMS and video-transmission even though a mobile-phone is in silent mode. Moreover, a device was able to restrict the detected-mobile-phone from accessing services through jamming which blocks the desired-frequency. However, the device was unable to discriminate two-distinct-phones operating in the same-frequency.

Kanwaljeet *et al* (2014), developed a line-follower-robot designated to detect the use of mobile-phones in restricted premises. When the robot detects RF-signals transmitted from the mobile-phone, it stops moving and sounds a beep-alarm and the LED blinks for notification until when RF-signals transmission stops. However, the robot cannot tell the exact location of the detected mobile-phone. The robot cannot rotate at any particular-angle which is less than 75 degree. To rotate less than 75 degree angle more sensors and programming would be needed.

A mobile-sniffer and jammer developed by Sujith *et al* (2014), has a capability to detect the use of GSM mobiles in examination halls and other "do not disturb"-areas. The sniffer-circuit consisted of RF-detector, GSM module and Peripheral Interface Controller (PIC). The device continuously detects the RF-signal level and produces a warning message when the RF-level increases.

All of the technologies outlined above have their-own-limitations; however, they also have a common factor, that all of them are quite-expensive, especially for developing-countries. This study is, therefore, focuses on cost-effective mobile-phone-detectors that will be affordable for educational institutions in developing countries.

3.2 Design of detectors

3.2.1 The mobile-phone-detection system (resistor-capacitor circuit)

The transmission-frequency of mobile-phones ranges from 0.9 to 3 GHz with a wavelength of 3.3 to 10 cm. A

circuit detecting gigahertz signals is required for a mobile bug. The construction of this small-size mobile-phonedetector is rather-simple and not expensive. For the construction to be understood and appreciated, a more-detaileddescription of the design is required using the diagrammatic- representations.

Ordinary LC (Coil-Capacitor)-circuits are used to detect low-frequency-radiation in the AM and FMbands. The tuned-tank-circuit having a coil and a variable-capacitor retrieve the signal from the carrier-wave. But such LC- circuits cannot detect high-frequency-waves near the micro-wave- region. Hence in the circuit, a capacitor is used to detect RF from mobile-phone considering that, a capacitor can store energy even from an outside source. Here the circuit uses 100 μ F disk-capacitors to capture the RF-signals from the mobile-phone. Figure 2 shows the circuit-diagram of mobile-phone-detector, while Figure 3 shows the assembly in operation (while LED is blinking), and Figure 4 shows the Breadboard- assembly of the mobile-phone-detector.

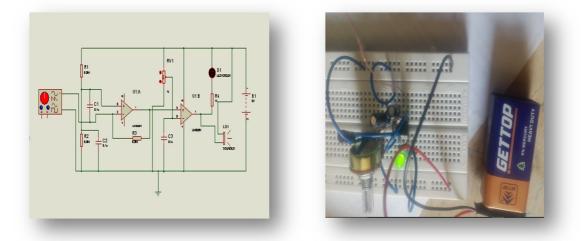


Figure 2: Circuit diagram of mobile-phone-detector Figure 3: Assembly in operation (LED blinking)

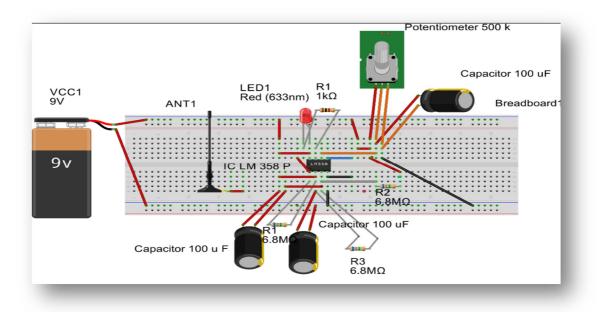


Figure 4: Breadboard-assembly of the mobile-phone-detector

A capacitor has two electrodes separated by a 'dielectric', like paper, and it can store energy and pass AC-signals. The 100uF capacitor is selected because it is a low-cost and has large-enough-capacity to accept energy from the mobile-phone-radiation. To detect the signal, the sensor-part should be like an aerial. There a natural-electromagnetic-field around the capacitor caused by the 50Hz from electrical-wiring. When the mobile-phone radiates high-energy-pulsations, capacitor oscillates and releases energy in the inputs of IC. This oscillation is indicated by the flashing of the LED or beeping of the Buzzer. In short, capacitor carries energy and is in an electromagnetic field. So a slight-change in field caused by the RF from phone will disturb the field and forces the capacitor to release energy. The black-wire of the battery is connected to the bottom-left of the board while the red-wire of the battery is connected to the bottom-right row of the board.

3.2.2. The Reed-switch-circuit-scanner

The basic reed-switch consists of two ferromagnetic-nickel-iron-wires and a glass-capsule. The two wires are formed into "reeds" by flattening one-end. The reed-ends are carefully aligned with a small overlap and then permanently sealed inside the glass capsule. The overlap or contact area of the reeds is coated with special metals (ruthenium). The nickel-iron-leads are tin-plated so that they can be soldered. The mobile-phone has a speaker which has a magnet hence magnetic field generated by the phone aids in its detection by this circuit. The two reeds act as magnetic-flux-conductors when exposed to an external-magnetic-field from either a permanent-magnet or an electromagnetic-coil. Poles of opposite-polarity are created at the contact-gap and the contacts close when the magnetic-force exceeds the spring-force of the reeds hence the lighting of LED (Light Emitted Diode) and the vibration of the Piezo Buzzer due to closed-circuit. The contacts open when the external-magnetic-field is reduced so that the magnetic-attractive-force between the reeds is less than the restoring- spring-force of the reeds hence the vibration stops and the Piezo-Buzzer too. Figure 5 shows the circuit diagram of the magnetic-Field-Circuit for Detection using Reed-Switches, while Figure 6 shows the Breadboard-assembly of the magnetic-Field-Circuit for Detection using Reed-Switches.

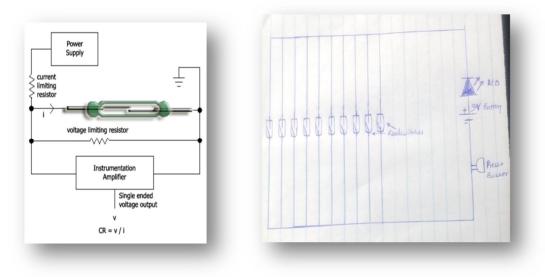


Figure 5: Circuit-picture of the magnetic- field-circuit for detection using Reed-Switches

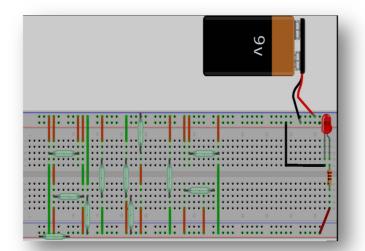


Figure 6: Breadboard-assembly of the magnetic- Field- Circuit for Detection using Reed-Switches

3.3 Testing of the two Devices

The design of both detectors was tested using a specified (under Material section) mobile-phone. The mobilephone was turned on and a phone-call was placed with the detector nearby. When mobile-phone receives the signal at the particular-place, the alarm makes the sound for indication of the mobile-phone presence and LED will glow for the indication. It was noticed that once the call was made and the detector detects the signal, the LED comes up along with the sound but shortly later on stops, even when the call was not aborted. After much troubleshooting, it was discovered that the antenna'-wire was fragile and a better-wire has to be used; finally the circuit was working successfully. Secondly, the display had LED which blinks due to presence of radio-frequency and the Piezo Buzzer vibrate as it produces sound. There was a variance in brightness of the LED depending on the distance between the device and the source of the radio frequency, the piezo responded to the variation in distance by producing high sound when the distance was reduced. The alarm continues until the signal transmission get off. The mobile-detector was found to be working at a radius of one meter. The device was able to detect incoming and outgoing phone-calls, messaging, and phone-video transmission, even if the mobile phone is kept in the silent mode.

The *reed detector* was able to detect the presence of mobile phone (via identification of the magneticfield in the speaker present in many-phones); the phone is detected even when the battery is removed or is switched off. The reed-switch would produce sound and the Led would light when a mobile-phone is detected. The range for the reed- switch, however, was only 1-5 cm. The reed-detector also could not detect some phones since they did not use magnetic field in their speaker, as they used piezoelectricity.

3.4 Estimated cost

The cost of the detectors was estimated via their respective Bill of Quantities, at the local retail-prices of 2016, assuming labor at 20% of the total-cost for their parts. The cost of the RF-detector, therefore, was established at 7USD, while the cost of magnetic-field-detector was around 3USD. In comparison with commercially-available-detectors (for example, USD 499 for PocketHound-model and USD 1, 650 for professional-surveillance one) the designed detectors could be considered as exceedingly cost-effective gargets.

4. Conclusion and recommendations

4.1 Conclusion

In this project an attempt was made to design two-systems, that will be used, independently, to detect mobilephones in the exam-venues: a mobile-detector with a range of 1.0m, using resistor-capacitor-circuit, which can detect both the incoming and outgoing-calls, as well as video-transmission and text messages, even if a mobilephone is kept at the silent mode; and a Reed-switch-circuit-scanner, which, responds to an applied-magnetic-field and, can be used to detect mobile-phones that are switched-off or put on flight-mode, and thus, it can be used to scan students (without physical-inspection) on their entering examination-rooms.

Advantages of the both systems are: It is small and compact in size, Portable and lightweight, Easy to handle and operate, Simple and easy to construct, Cost-effective, with Less power consumption.

Potential Applications: it can be used to prevent use of mobile-phones in examination halls, and for detecting the use of mobile-phones for spying and unauthorized video-transmission; it is also useful where the use of mobile-phone is prohibited or restricted; in particular, it can be used for military and civil defense purposes to detect mobile phones (subject to increasing its radius of operation- range), and it can be used in hospitals and airplanes where, mobile signals interfere with the electronic-equipment, which may have fatal-consequences.

Overall, the results of this concise study, is rather optimistic, providing a good starting point for advanced investigations and improvements of the same.

4.2 Recommendations

Regarding cheating at exams: The emergence of e-cheating has added to the challenges of conducting credible and reliable-examinations. The way forward is a holistic-approach involving all stakeholders, using technological and non-technological-solutions. A prevention approach that involves developing students as individuals, who do not want to cheat and providing an environment that discourages cheating is the best-option. Periodic-enlightenment-campaigns, on the harms of cheating, should be carried out by examination-bodies and university'-authorities.

Engineering-approach involves an installation of detection-devises that could indicate whether a mobilephone is being operated within an examination-hall. The policeman approach entails monitoring and enforcement of laws and regulation guiding an examination i.e. using a mobile-phone-scanner to detect a mobile-phone at the entrance of examination room. Monitoring and enforcement involves proper-invigilation, apprehending and appropriate sanctioning of defaulters. The sanctioning of defaulters will serve as restraint to others. *Regarding mobile-phone-detectors developed in this study:*

Future-research is considered necessary in the following areas: (1) the range of operation of the RF-detector can be extended to a wider area, say up to 15m. Mobile bug incorporating 'MEMS (micro-electro-mechanical systems)' technology and sensors can be used for that purpose;(2) it can be modified to detect signals in a particular-direction and identify exact-position of an active-mobile-phone (where cell-phones of faculty members in examination-halls are switched-off, so that only students' phones can be traced out), for that purpose the detector should be programmed; (3) Current-systems are designed only for 2G/3G structure, hence a 4G-complaisants can be developed; (4) Being able to detect Bluetooth transfers is also advisable; and finally, (5) to research on possibilities

of detecting mobile-phone, even when all mobile-operators are switched-off and, therefore, "no-network" indicated on that particular phone, as this tactics is used by students to retrieve information, relevant to exam, which was uploaded before-hand, on their mobile-phones.

5. Acknowledgements

The authors wish to express gratitude to the technical-staff of the Electrical Laboratory of ECE, SOE for providing necessary-facilities for this concise-unfunded-study, and to Potas Achola and Sharon Atambo for their-valuable-assistance in conducting experiments and validation of the system.

References

- Ajasa, A.; Shoewu, O. and Nwamina, P. (2014). "Design and Development of a Mobile Phone Signal Detector", *Pacific Journal of Science and Technology*, 15(2):167-172.
- Alonge, M. (2003). Assessment and Examination: the Pathways to Educational Development, 9th Inaugural Lecture. Ado-Ekiti: Ekiti State University.
- Blurton, C. (2002). New Directions of ICT Use in Education. [Online] Available: http://www.unesco.org/education/educprog/lwf/dl/edict.pdf (June 10, 2016).
- Bruno, U and Ibid, I. (2012). "The Counseling Implications of Examination Malpractices among University Undergraduates", *Research Journal of Organizational Psychology and Educational Studies*, 1 (2), 199–202
- Blog- jammer-store [Online] Available: www. Blog.jammer-store.com/2009/11/how-mobile-jammers work, (June 10, 2016).
- Curran, K.; Middleton, G. and Doherty, C. (2011). "Cheating in Exams with Technology", *International Journal* of Cyber Ethics in Education, 1(2), 54-62, April-June 2011.
- Ismaila, A.; Onche, O.; Muhinat, B. and Hassan, I. (2012). "A Survey of University of Ilorin Students' Use of Mobile Phone in Lecture rooms and its Implications in Education for Nigeria Development", *Journal of Education and Practice*, Vol 3, No 10, 2012.
- Kanwaljeet, S.; Mandeep, S. and Gupta, N. (2014)."Design and Implementation of Cell-Phone Detection based Line follower Robot", *International Journal of Electronics and Computer Science Engineering*, Volume1, Number 3.
- Lawal, W.; Akinrinmade, A. and Ijarotimi, O. (2013). "Effects of Unrestricted Mobile Phone Usage in Selected Public Places in Nigeria: A Case Study of Akure", *International Journal of Science and Research (IJSR)*, Volume 2 Issue 5, May 2013.
- Masri, A. (2015)."Using Mobile Phone For Assessing University Students In English Literature In Jordan", *European Scientific Journal*, October edition vol. 8, No.24, 2015.
- Mbaocha, C. (2012). "Design and Implementation of Intelligent Mobile Phone Detector", *Academic Research International*, Vol. 3, No. 1, July 2012.
- Mohan, D. (2012). "Novel Mobile Detector Sensing Alarming and Reporting System", *ARPN Journal of Science and Technology*, VOL. 2, NO. 1, January 2012.
- Nyamawe, A. and Mtonyole, N. (2014). "The Use of Mobile Phones in University Exams Cheating: Proposed Solution", *International Journal of Engineering Trends and Technology (IJETT)*, Volume 17, Number 1, Nov 2014.
- Okebukola, P. (2014). "Contemporary Use of Mobile Devices for Cheating During Examinations", [Online] Available: www.ijern.com, (June 10, 2016).
- Shon, P. (2006). "How College Students Cheat On In-Class Examinations: Creativity, Strain, and Techniques of Innovation", [Online] Available: http://hdl.handle.net/2027/spo.5240451.0001.010 (June 11, 2016).
- Styron, J. and Ronald, A. (2010). "Student Cheating and Alternative Web-Based Assessment", *Journal of College Teaching & Learning* May 2010 Volume 7, Number 5.
- Sujith, M.; Bibin, J.; Anoop, P. and Dileep, J. (2014). "Mobile Sniffer and Jammer", *International Journal of Research in Engineering and Technology*, Volume: 03 Special Issue: 01.
- "Wolfhound Cellphone Detector" (N.A) (2013). Berkeley Varitronics System. [Online] Available: http://www.busystems.com, (June 10, 2016).
- Yee, K. and MacKown, P. (2014). "Detecting and Preventing Cheating During Exams", [Online] Available: www.syr.edu/gradschool/pdf/resourcebooksvideos/AIBook/AIYee.pdf, (June 12, 2016).