

Design and Testing of a Mobile-Phone-Jammer

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

Abstract
Dissimilar cellular-systems process signals differently, and yet, all cell-phone-networks use radio-signals that can be interrupted or, even, blocked, completely. This project highlights the design of a simple, low-cost mobile-phone-jammer and aims to present a solution for the problem of inappropriate-use of the cell-phones in restricted and prohibited-areas. The main concept of jamming is the releasing of signal (noise) of the same-frequency which is using by mobile-service-provider to overpower and destruct the user-signal. The fabrication of the jammer involved uncomplicated discrete components, resistors, capacitors, inductors and transistors to generate the required frequency (*noise*) and then amplifies the frequency generated to range of 800 MHZ to 1.4 GHZ in order to match the frequency of the mobile-phone being transmitted by the base-station. Relatively-satisfactory-jamming of a mobile-signal was confirmed by the blocking of the signals of the mobile-phones in 2G and 3G-networks (UMTS / WCDMA) operated via Safaricom, Airtell, Orange, and YU service-providers, when the phone indicated "*no network*", thereby allowing no call to go through, with no-interference to other communication-means observed. Overall recommendation is that further and more deeper-research is needed to produce more-sophisticated and better jamming devices, as not to affect the other base-station-transmission-systems.
Keywords: mobile, phone, jammer, design, signal.

1. Introduction
Relevant and important-background-topics will be highlighted in this-section.

1.1. Cellular- phone technology
Cell-phones receive their signals from a base-station, which consist of a tower and a small-building containing the radio-equipment. The transmission of RF-signals is possible due to the cellular-approach, where a city/town is divided into cells. Cell is typically the area (several-kilometres) around a tower in which a signal can be received. A large-number of base-stations in a city/town of any-size is required; a typical-large-city can have hundreds of towers. But because so many-people are using cell-phones, costs remain relatively low-per-user. Each-carrier in each-city also runs one central-office called the Mobile Switching Centre (MSC), which handles all of the phone-connections to the normal land based phone-system, and controls all of the base-stations in the region (Miao, 2016).

Division of a city into small-cells allows extensive-frequency-reuse across the area, so that millions of people can use cell-phones simultaneously. Cell-phones operate within cells, and they can switch cells as they move around. Cells give cell-phones incredible-range; someone using a cell-phone can drive hundreds of kilometers and maintain a conversation the entire-time due to the cellular-approach and the GSM RACH (random access scheme), which is relatively-straightforward (when a request for connection is not answered, the mobile-station will repeat it after a certain-interval. The maximum-number of repetitions and the time between them is broadcast-regularly. After a MSC has tried to request service on RAC Hand has been rejected, it may try to request service from another cell). The MSCs are also linked to several-databases called Home Location Registers (HLR) that contain the information of each cell-phone-subscriber. The HLR has the capacity to track the geographical-location of all the cell-phones that are covered under the area of that particular MSC (Prensky, 2001). Each-cell has a base-station; Figure 1 shows the cells- arrangement.

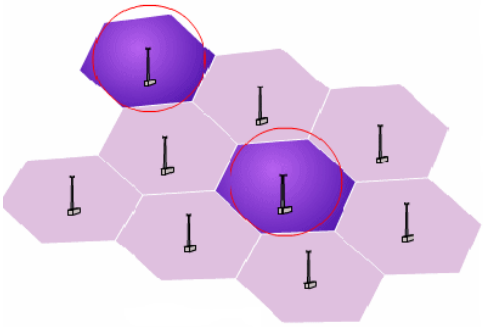

Figure 1: Cell-arrangement

When a cell-phone is turned-on, it reaches the nearest base-station and establishes a communication-

link and this process is called 'Registration'. The three-main-technologies used by cellular-phone providers are 2G, 3G, and 4G. Each-generation of technology uses a different-transmission-protocol. The transmission protocols dictate how a cellular-phone communicates with the tower. Some examples are: Frequency division multiple access (FDMA); Time division multiple access (TDMA); Code division multiple-access (CDMA); Global system for mobile communications (GSM) CDMA2000; Wideband code division multiple-access (WCDMA), and Time-division synchronous-code-division-multiple-access (TD-SCDMA) among others (Miao, 2016).

A cell-phone is a full-duplex-device, meaning that it operates on two frequencies; one-frequency is used for talking and a second, separate-frequency, is for listening, enabling both-people on the call to talk at once (Gralla, 2002).

A single-cell in an analog-cell-phone-system uses one-seventh of the available-duplex-voice-channels. That is, each-cell is using one-seventh of the available-channels so it has a unique set of frequencies and there are no collisions; a cell-phone-carrier typically gets 832 radio-frequencies (56 channels) to use. Analog-cellular-systems are considered first-generation-mobile-technology, or 1G. With digital transmission methods (2G), the number of available-channels increases. For example, a TDMA based digital system (more on TDMA later) can carry three-times as many-calls as an analog-system, so each cell has about 168 channels-available. Cell-phones have low-power-transmitters in them. Many cell-phones have two-signal-strengths: 0.6 watts and 3 watts. The base-station is also transmitting at low-power. Low-power transmitters have two advantages: The transmissions of a base-station and the phones within its cell do not make it very far outside that cell. Therefore, 2 different-neighboring-cells can reuse the same-frequencies extensively across their limited-area (Prensky, 2001).

The power-consumption of the cell-phone, which is normally battery-operated, is relatively-low. Low-power means small-batteries, and this is what has made hand-held cellular-phones possible. Mobile-phones have an internal-memory called Number Assignment Module (NAM). Each NAM has its-own Mobile Identification Number (MIN) programmed into it, which is a wireless-phone-number. The phone also contains an Electronic Serial Number (ESN), which acts as recognition for the phone and helps as a security against cell-phone fraud. A number identifying the cell phone with which it works is called the System ID (SID) (Gralla, 2002).

Cell-phones provide an incredible array of functions. Depending on the cell-phone model, one can: Store contacts-information, Make task or to-do lists, Keep track of appointments and set reminders, Use the built-in calculator for simple math, Send or receive e-mails, Get information (news, entertainment, and business-updates) from the internet, record and view a video or an audio-data, Play games, Watch TV, Send and receive text messages, and Integrate other devices such as PDAs, MP3 players and GPS receivers among others (Fielden & Malcolm, 2008). It is evident that the positive purposes of mobile-phones have added tremendous-comforts and conveniences to our-living.

1.1.1 Analog-cell-phones (first- generation)

In 1983, the analog-cell-phone standard called AMPS (Advanced-Mobile-Phone-System) was approved by the Federal Communication Commission, USA and first used in Chicago. AMPS use a range of frequencies between 824 megahertz (MHz) and 894 MHz for analog-cell-phones. In order to encourage competition and keep prices low, governments required the presence of two-carriers in every-market, known as A- and B-carriers. One of the carriers was normally the local-exchange carrier (LEC)-a local-phone-company. Carriers A and B are each assigned 832 frequencies: 790 for voice and 42 for data. A pair of frequencies (one for transmit and one for receive) is used to create one channel. The frequencies used in analog-voice-channels are typically 30 kHz wide; 30 kHz was chosen as the standard-size because it gives voice- quality comparable to a wired-telephone. The transmitting and receiving-frequencies of each-voice-channel are separated by 45 MHz to keep them from interfering with each-other. Each carrier has 395 voice-channels, as well as 21 data channels to use for house-keeping-activities like registration and paging. AMPS and NAMPS only operate in the 800-MHz-band and do not offer many of the features common in digital- cellular-service, such as e-mail and Web-browsing (Campbell & Park, 2008).

1.1.2 Digital- cell-phones (second- generation)

Digital- cell-phones use the same-radio-technology as analog-phones, but they use it in a different-way; Analog-systems do not fully-utilize the signal between the phone and the cellular-network; analog-signals cannot be compressed and manipulated as easily as a true digital-signal. Digital-phones convert a voice into binary-information (1s and 0s) and then compress it. This compression allows between three and 10 digital cell-phone-calls to occupy the space of a single-analog-call. Many digital-cellular-systems rely on frequency-shift-keying (FSK) to send data back and forth over AMPS. FSK uses two-frequencies, one for 1s and the other for 0s, alternating rapidly between the two to send digital-information between the cell-tower and the phone. Clever-modulation and encoding-schemes are required to convert the analog-information to digital, compress it and convert it back again while maintaining an acceptable-level of voice-quality; hence, digital-cell-phones have to contain a lot of processing power (Fielden & Malcolm, 2008). Old-fashioned-analog-cell-phones and today's digital devices are equally susceptible to jamming, therefore mobile-phones of both generations are to be used in

the testing of the jammer.

1.2. Inappropriate use of the mobile-phones

Communication is the unseen-filament that connects and unites people. The modern-digital-environment presents an exceptional array of possibilities for communication, interaction, and information-retrieval, at the fingertips, that was never-before-available (Akaiwa, 2007).

It is well-known-fact, that the mobile-phones, although having huge-range of benefits for the society, now, also have become a device used for committing crimes (under some-circumstances), and have made adverse-effect on the stability of our-global-society (Campbell & Park, 2008). With the development of science and technology, tracking and surveillance of mobile-phones have become the most-important inspection-method and information-source in every-country. As a result, as long as carrying a mobile-phone; whenever one use it or not, it is possible to cause secret-information-leakage, even at stand-by-mode, bringing a real-danger to yourself, to your-family, to your-business, to your-office, or even to your-political-party and the country at large. In addition, using-mobile phones at petrol-station or oil-depot would expose one to the physical-danger, as it can cause fire or blast, which brings serious- consequences. Terrorists and hostiles use mobile-phones to remotely-activate fire-bombs and other-malicious-activities, such as recruiting youngsters into Al-Shabaab, Isis and alike. Using mobile-phone while driving is another-form of its-inappropriate and potentially-dangerous-use; according to Cohen & Graham (2003), the leading-cause of crashes is failure to maintain-attention, as some-drivers talk on cell-phones send text messages while driving, which brings a real-danger to themselves and to the other road-users. Illegal-use of mobile-phones in by prisoners is another global-concern.

On the other hand, some students use mobile-phones to cheat at the exams. National-poll on the use of digital-media for cheating in exams, conducted by the Benenson Strategy Group, revealed that almost ¼ of high school and university students surveyed said they did not think storing notes on a cell-phone or texting during an exam constituted cheating. More than 35% of students admit to cheating with cell-phones, and more than half admit to using the Internet to cheat. More importantly, many students do not consider their-actions to be cheating at all. Other key-findings from the poll include: 41% of students say that storing notes on a cell-phone to access during a test is a serious-cheating-offense, while 23% do not think it constitutes cheating at all; 45% of students say that texting friends about answers during tests/exams is a serious-cheating-offense, while 20% say it is not cheating at all; 76% of parents say that cell phone-cheating happens at their children' schools, but only 3% believe their own-children have ever used a cell-phone to cheat; 62% of students with cell-phones use them during classes, regardless of school-policies against it; and students with-cell phones send and receive on average 400 text-messages a week and 110 a week, while in the classroom (Daily Nation, 2014). The results highlight a real-need for parents, educators, and leaders to start a discussion on digital-ethics and to find new-ways to fight the current-threat of inappropriate-use of mobile-phones.

1.3. Purpose of the study

It is excellent to be able to call anyone, 24/7, and all around the globe. Unfortunately, restaurants, movie-theaters, concerts, shopping-malls, hospitals, banks, libraries, and churches all do suffer from the spread of cell-phones because not all cell-phone-users recognize, or make any account, that it could be a restricted for mobile-use-area, or, even if they understand that the use is restricted, still, they cannot control themselves and keep-on talking and talking, sometimes, for a long-time; in addition, some of them do talk very-loudly, making a whole-experience of listening to that mobile-conversation (as outsider's point of view) as annoyance and unnecessary-interruption, and particularly disturbing because silence, peace or concentration is expected. The fact is, with the use of cell-phones, people sometimes lose the capacity to manage the boundaries between appropriate and inappropriate usage (Ling, 1997).

It is a nuisance when a phone rings in a church, mosque or in a private-meeting, however, it is even-more worrying and, even, dangerous, when mobile-phones are illegally-used by inmates in prisons to conduct and arrange their criminal-activities.

In the-recent-past, seminars and conferences-organizers are also constantly complaining having a hard-time begging people to turn-off their-phones, while sessions are ongoing, this even has led to many posters on the walls showing mobile-phone crossed in red. Terrorist have also advanced from suicide-bombers to mobile-phone-detonation because nearly every-populated- place in the world has cell-phone coverage, making it easy to detonate a bomb from any location in the world as long as there is some network coverage. An RF-jammer would be very indispensable in such occasions.

On the other hand, cases of students cheating at exams are widespread and on the increase locally and globally. A total of 5,101 of 2015 KCSE exam-candidates will not get their results because they cheated. According to the results released by the Education Minister of Kenya, there are increased cases of examination malpractices compared to 2014, when there were 2,975 cases. Out of 47 Kenyan-counties, only one-Isiolo County has no cheating case. The reasons given by the Minister is that the exam was leaked through the use of

mobile-phones. Students would make calls to fellow-students, send short message service (sms) or send images of question-papers via the internet (Nation, 2016). Referring to the idea of embodiment of mobile-phones in every-day-life and learning-process of our youths, Prensky (2005) cites the direct-words of a Japanese student who said, "if you lose your mobile-phone you lose part of your- brain". Some-students, being-crafty, have always found ways to cheat, but the tools they have today, in the 24/7-media-world, are more-powerful than ever; therefore new and more-advanced-solutions should be discovered to keep in touch with the reality. The cheating exams and other inappropriate use of the mobile-devises could be avoided if radio-frequency-jammers were used. These-factors have motivated the researches to make a simple-mobile-signal-jammer. The objectives of this study is: to design a jammer-system that prevents mobile-phones use in a particular radius (jamming signals), and to block mobile-phone use by sending radio-waves along the same-frequencies that mobile-phones use thereby causing interference with the communication-towers.

1.4. Tool to address the problem - Mobile-Phone-Jammer

The word "jamming" is defined as the deliberate-transmission of interfering-signals to disrupt the normal-operation of mobile-phones. Radio-jamming is the deliberate radiation, re-radiation, or reflection of electromagnetic-energy for the purpose of disrupting use of electronic-devices, equipment, or systems – in this case, mobile devices such as cell-phones, which emit radio-frequency (RF), as any of the electromagnetic wave-frequencies that lie in the range extending from around 3 kHz to 300 GHz, which include those frequencies used for communications or radar-signals. Any-transmitter, apparently, has the potential to cause interference to other-radio-services. Simply put, jammers are transmitters that are specifically designed to disrupt cellular and other-mobile-devices.

A mobile-phone-jammer is a device that obstructs transmission and receiving of radio-frequency to and from a mobile-phone with a base-station. When used, the jammer effectively disables cellular-activity between the base-station and the device, by creating a temporary "dead-zone" to all cell-phone-traffic in their-immediate-proximity. Mobile-Phone-Jammers were originally developed for the law-enforcement and the military to interrupt communications by the enemies, criminals and terrorists. Some were also designed to outwit the use of certain-remotely-detonated-explosives. Nowadays, the mobile-jammer-devices are becoming civilian products rather than electronic-warfare-devices, since with the increasing number of the mobile-phone-users the need to disable mobile-phones in specific-places where the ringing and use of cell-phone would be disruptive, has increased. These places include worship-places, university lecture rooms, libraries, concert halls, meeting rooms, banks, and other places where silence is appreciated. The civilian-applications were apparent, so over-time, many-companies originally-contracted to design jammers for government-use switched-over to sell these-devices to private-entities. Since then, there has been a slow but steady-increase in their purchase and use, especially in major-metropolitan areas (Zorn, 2011).

Mobile-jammers use a technique commonly-referred to as denial-of-service attack. Here, jamming-devices will transmit-radio-frequencies similar that of a cell-phone but of greater-power hence will disrupt the communication between the phone and the cell-phone-base-station in the tower. Disrupting a cell-phone is the same as jamming any other type of radio-communication (Mahato& Vimala, 2015). The Output Power of the Jammer can typically be stated in Watts or in some cases dBm. The radius of cell-phone-jammers can range from a few meters for pocket models to kilometers for more-sophisticated-units (Gopal, 2013).

The technique used in most of the commercial-jammers is based on noise-attack. In the previously-designed cell-phone-jammers, designers came up with an electronic-device that acts as a transmitter to transmit electromagnetic- signals of respective-frequency and higher-power as used by GSM-systems (Global System for Mobile Communications, originally Groupe Spécial Mobile). In this-technique voltage controlled-oscillator (VCO) plays a major-role in generating the jamming-frequency. In this-research, it was found that the above-technique is rather-complex, therefore in this study the idea of jamming through simple-circuitry (using capacitors, inductors and resistors) was used, which potentially simpler, easier to fabricate and generally more-economical. Cell-phone-jamming-devices are an-alternative to more expensive-measures against cell-phones, such as Faraday-cages, which are mostly suitable as in-built -protection for large-structures (MPCC, 2003).

Other-jamming-techniques are described as follows: (ACA, 2003).

1. *Type "A" Device (Jammers):* This type of device comes equipped with several independent-oscillators transmitting 'jamming signals' capable of blocking frequencies used by paging devices as well as those used by cellular-systems-control-channels for call-establishment.

2. *Type "B" Device (Intelligent-Cellular-Disablers):* Unlike jammers, Type "B" devices do not transmit an interfering-signal on the control-channels. The device, when located in a designated 'quite' area, functions as a 'detector'. It has a unique-identification-number for communicating with the cellular-base-station.

3. *Type "C" Device (Intelligent-Beacon-Disablers):* Unlike jammers, Type C devices do not transmit an interfering-signal on the control channels. The device, when located in a designated 'quiet' area, functions as a 'beacon' and any compatible-terminal is instructed to disable its ringer or disable its operation, while within

the area of beacon.

4. *Type "D" Device (Direct Receive & Transmit Jammers):* This jammer behaves like a small, independent and portable base station, which can directly interact intelligently with the operation of the local-mobile-phone. The jammer is predominantly in receiving-mode and will intelligently-choose to interact and block the cell-phone directly if it is within close-proximity of the jammer.

5. *Type "E" Device (EMI Shield - Passive Jamming):* This technique is using EMI suppression techniques to make a room into what is called Faraday-cage. Although labour-intensive to construct, the Faraday-cage essentially blocks or greatly attenuates, virtually all electromagnetic-radiation from entering or leaving the cage.

Type "A" Device (Jammers) will be the subject of this study.

Jamming-devices overpower the cell-phone by transmitting a signal on the same-frequency. The power of the signal should be high-enough so that the two-signals collide and cancel each-other-out. Cell-phones are designed to add power if they experience low-level-interference, so the jammer must recognize and match the power-increase from the phone. Some-jammers block only one of the frequencies used by cell-phones, which has the effect of blocking-both. The phone is tricked into thinking there is "no service" because it can receive only one of the frequencies. Less-complex-devices block only one group of frequencies, while sophisticated jammers can block several-types of networks at once to head off dual-mode or tri-mode-phones that automatically switch among different-network-types to find an open-signal. Some of the high-end-devices block all-frequencies at once, and others can be tuned to specific-frequencies (Miao, 2016).

To jam a cell-phone, one need, is a device that broadcasts on the correct frequencies. Although different-cellular- systems process signals differently, all cell-phone-networks use radio-signals that can be interrupted. GSM, used in digital-cellular and PCS-based systems, operates in the 900-MHz and 1800-MHz-bands in Europe, Asia and Africa in the 1900-MHz (sometimes referred to as 1.9-GHz)-band in the United States of America. Jammers can broadcast on any frequency and are effective against AMPS, CDMA, TDMA, GSM, PCS, DCS, iDEN and Nextel-systems. The actual-range of the jammer depends on its power and the local-environment, which may include hills or walls of a building that block the jamming-signal. Low-powered-jammers block calls in a range of about 30 feet (9 m). Higher-powered units create a cell-free-zone as large as a football-field (around 120mx90m). Units used by law-enforcement can shut-down service up to 1 mile (1.6 km) from the jammer-device. A portable mobile-phone- jammers featured by the Universal and Handheld Design, could block worldwide cell phone networks within 0.5-10 meters, including GSM900MHz, GSM1800MHz, GSM850MHz/CDMA800MHz and also 3G networks (UMTS / WCDMA) (Zorn, 2011).

There are, basically, two types of jammers: *The-first-type* is usually smaller-devices that block the signals coming from cell- phone-towers to individual-cell-phones, and it can block signals within about a 30-foot (9m) radius. Cell-phones within this range simply show no signal. *The- second- type* of cell phone-jammer is usually much-larger in size and more-powerful. They operate by blocking the transmission of a signal from the satellite to the cell-phone-tower (Mahato &Vimala, 2015). The-first-type jammer will be the subject of this design.

Mobile-phone-jammers can be also customized, depending on the area of application and the reason behind the jamming. They can be grouped as follows: cell-phone-jammer-for leisure and general-purpose-work; Portable-cell-phone- jammer; Remote-control-cell-phone-jammer – where jamming does not necessary have to be from the area where the device is located; Adjustable-cell-phone-jammer; School & prison-phone-jammer - to prevent cheating in examinations and destructions during lectures as well as illegal use in prisons; Explosion-proof cell- phone- jammer - to curb RF-triggered bombs; and Police & military phone-jammer -to prevent illegal-activities like by kidnappers trying to extort money from citizens or criminals planning an illegal activity (Gopal, 2013). This-design is focused on the School & prison-cell-phone-jammer.

2. Materials and Methods

2.1 Methods

2.1 1. Jammer-circuit

For any jammer-circuit, there are three main-important-functional parts, and when they are combined together, the output will work as a jammer. There are: (1) RF-amplifier; (2) Voltage-controlled-oscillator; and (3) Tuning-circuit. Figure 2 shows the self-explanatory flow-chart of the operation of the mobile-phone-jammer. The EdrawSoft- Electrical-Drawing-Software was used for creating the circuit of the mobile-phone-jammer.

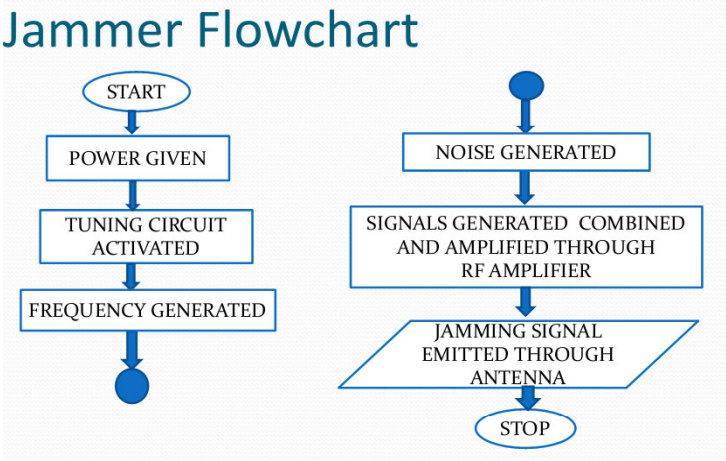

Figure 2: Sequential-mode of operation of the mobile-phone-jammer.

2.1 2. Jamming Techniques

The three-common-ways of jamming a radio-frequency are: *Denial of Service, Shielding Attacks, and Spoofing.*

Denial of Service (the device transmits a noise-signal at the same-operating-frequency of the mobile-phone in order to decrease the signal-to-noise-ratio (SNR) of the mobile under its minimum-value, thereby disrupting the communication between the phone and the cell-phone-base-station. This kind of jamming-technique is the simplest one since the device is always on). *Shielding Attacks* (This is known as TEMPEST or EMF-shielding. This kind requires closing an area in a Faraday-cage so that any-device inside this cage cannot transmit or receive RF-signals from the outside of the cage. This area can be as large as buildings or a football pitch), and *Spoofing* (the device forces the mobile to perform a self-shut down. It very- difficult to be implemented since the jamming-device should first detects any mobile-phone in a specific area, and then the device sends the signal to disable the mobile-phone. Some types of this technique can detect if a nearby-mobile-phone is there and sends a message to tell the user to switch the phone to the silent-mode). Denial of Service Technique is used in this project.

2.1 3. Design-Parameters

Based on the design-considerations, the device is transmitting signal (noise) on the same frequencies of the two bands GSM 900 MHz, and GSM 1.8 GHz (known also as DCS 1800 band). Selected design- parameters have to be determined first to establish the device-specifications. These parameters are as follows:

The distance to be jammed (D): This parameter is very-important in this-design, since the amount of the output power of the jammer depends on the area that needed to be jammed. The design is established upon D=10 meters for DCS 1800-band and D=20 meters for GSM 900-band.

The frequency bands: In Kenya, the mobile-network operates on the 900 MHz, 1800 MHz (2G), and 2 GHz (3G) GSM-bands like most- European-carriers. Since 2014, 4G is available in limited areas in Nairobi and Mombasa (CCK (2015).

GSM900 (Uplink: 890-915 MHz; Down link: 935-960 MHz); DCS 1800 (Uplink: 1710-1785MHz-1785 MHz; Downlink: 1805-1880 MHz). In this-design, the jamming-frequency must be the-same as the downlink, because it needs lower-power to do jamming than the uplink-range and there is no need to jam the base station itself. Thus, the design-frequency will be as follows: GSM 900 935-960 MHz and GSM 1800 1805-1880 MHz

Jamming–to-signal ratio {J/S}: Jamming is successful when the jamming-signal denies the usability of the communication-transmission. In digital-communications, the usability is denied when the error-rate of the transmission cannot be compensated by error-correction. Usually, a successful-jamming-attack requires that the jammer-power is roughly equal to signal-power at the receiver (mobile-device). The general-equation of the jamming-to-signal ratio is given as follows (Tata, 2015).

$$J/S = (PjGjrGrjRtrLrBr) / (PtGtrGrtRjrLjBj)$$

Where:

Pj = jammer power
Pt = transmitter power
Gjr = antenna gain from jammer to receiver
Grj = antenna gain from receiver to Jammer
Gtr = antenna gain from transmitter to receiver
Grt = antenna gain from receiver to transmitter
Br = communications receiver bandwidth
Bj = jamming transmitter bandwidth

Rtr = range between communications transmitter and receiver
Rjt = range between jammer and communications receiver
Lj = jammer signal loss (including polarization mismatch)
Lr = communication signal loss

For GSM, the specified system SNR min is 9 dB which will be used as the worst-case-scenario for the jammer. The maximum-power at the mobile device Pr is -15 dBm.

Free space loss {FSPL} (or path loss) is given by the following-formulae (Tata, 2015).

$$\mathrm{FSPL(dB)} = 10\log_{10}\left(\left(\frac{4\pi df}{c}\right)^2\right)$$

Where:

λ = the signal wavelength (in meters),
f = the signal frequency (in hertz),
d= the distance from the transmitter (in meters),
c= the speed of light in a vacuum, 2.99792458×10^8 meters per second.

The maximum-free-space- loss (worst-case F) happens when the maximum-frequency is used in the above-equation. Using 1880 MHz gives: F (dB) =32.44+20 log 0.01 + 20 log 1880 which gives F =58 dB.

Power calculations: The power that is needed to be transmitted to jam any-cell-phone within a distance of around 10 meters for DCS should be determined. From the above considerations, the required-output-power from the device, as follows: Using SNR=9 dB and the maximum-power-signal for mobile-receiver = -15 dBm, gives J = - 24 dBm. But, our goal is to find the output power from the device, so when we add the free space loss to the amount of power at the mobile receiver we get our target: Output power = -24dBm+58dB = 34 dBm

2.1 4. Components of Jamming Device

Main components are: Power Supply, Circuitry, and an Antenna. In addition, the jammer must have an on/off switch and a light that indicates it is on or off.

2.1 4. 1. Power Supply

The power supply consists of the following main parts as shown in Figure 3, followed by brief description of the same.

Figure 3: Power supply of the jammer

Transformer (used to transform the 220VAC to other-levels of voltages); *Rectification* (used to convert the AC voltage to a DC one. There are two methods for rectification: Half wave-rectification, where the output-voltage appears only during positive-cycles of the input-signal and Full wave-rectification, where a rectified output- voltage occurs during both the positive and negative-cycles of the input-signal); *The Filter* (used to eliminate the fluctuations in the output of the full wave rectifier (to eliminate the noise) so that a constant DC-voltage is produced); and *Regulator* (regulates the amount of voltage entering the circuit components).

2.1 4. 2. Circuitry

Any jammer-circuit is consists of minimum of four-main-circuits. When they are combined together, the output of that circuit will work as a jammer. There are: Voltage-controlled oscillator, Tuning circuit, Noise-generator, and RF-amplification unit (Zorn, 2011). Following is a concept of the operation for each.

a) *Voltage Controlled Oscillator (VCO)* is an electronic-oscillator whose oscillation-frequency is controlled by a voltage-input. The applied-input-voltage determines the instantaneous oscillation frequency. Consequently, modulating- signals applied to control-input may cause frequency modulation (FM) or phase-modulation (PM). A VCO may also be part of a phase-locked-loop. VCO is the most-important among other parts in this jammer-circuit. It is like the heart of the jammer. VCO produces RF-signal which will interact and interfere with the cell- phone-device. The output of the VCO has a frequency which is proportional to the input-voltage, thus, the output-frequency can be controlled by changing the input-voltage. The size of the VCO will depend on whether one is trying to create a desktop-mobile-phone-jammer or a portable- handheld- jamming- device. In this project, emphasis is on a small, portable jammer.

b) Tuning Circuit can be of two types: open-loop and feedback. *Open-loop* is quite simple and requires just a few op-amps with additional-passive-components. It is a saw-tooth wave-generator which makes VCO to go from lowest to highest-frequency. The feedback is using PLL (phase-locked-loop) to adjust the VCOs-frequency constantly. *Feedback*, on the other hand, requires the presence of a feedback-loop. It is a regenerative-circuit allows an electronic-signal to be amplified many-times by the same-active-device. It consists of an amplifying-vacuum-tube or transistor with its output connected to its input

through a feedback-loop, providing positive- feedback. This-circuit was widely-used in radio-receivers, called regenerative-receivers. Open-loop type was used in this study.

c) Noise- Generator produces random-electronic-output in a specified-frequency-range to jam the cell-phone network-signal (part of the tuning-circuit). In the circuit two-capacitors connected in parallel are used to generate the electronic-pulses in some-random-fashion (technically-called-noise) which are then combined with frequency generated by the tuned- circuit, amplified and transmitted to the air to jam the corresponding-signal. The noise will help in masking the jamming-transmission, making it look like random "noise" to an outside-observer. Without the noise-generator, the jamming-signal is just a sweeping, un-modulated continuous-wave-RF-carrier.

d) RF- Amplification- Unit is used to increase the area covered by the jammer along with its signal-blocking-power. The more-power has the signal-blocker, the bigger radius it jams. More-power equals less-time for battery to live. The RF-amplifier in this circuit will amplify the signal generated by the tuned-circuit. The amplified-signal is given to the antenna through a capacitor which will remove the DC and allow only the AC signal to be transmitted in the air.

2.2. Materials

The components used for the jammer, including their- relevant- details are shown in Table 1.

In addition, transmitting-antenna is necessary, as most-important-part of any-transmitter. In order to have optima-power-transfer, the antenna-system must be matched to the transmission-system. The main-characteristic of antenna is VSWR (Voltage-Standing-Wave-Ratio). The antenna should have VSWR of 3 or lower, because the return-loss of this antenna is minimal. The antenna used in the project is λ/4 wave monopole-antenna and it has 50 Ohm impedance so that the antenna is matched to the transmission system. Also this antenna has low VSWR of 1.7, and a bandwidth of 150MHz around 916 MHz center- frequencies which cover the mobile-jammer-frequency-range. The antenna gain is 2dBi.

Table1: Parts list

Component No and name		Value	Usage
R1	resistor	100R	Emitter loading
R2	resistor	39k	Base Biasing
C1	capacitor	15 pf	Frequency Generating
C2	capacitor	4.7pf	Feedback
C3	capacitor	4.7pf	Feedback
C4	capacitor	102pf	Noise Reduce
C5	capacitor	1MF	Coupling
C6	capacitor	2.2pf	Coupling
C7	capacitor	103pf	Decoupling
Q1	transistor	BF 494	Amplification
L1	inductor	22nH	Frequency Generating

Before linking all to the antenna, power-supply shall not be switched-on at first; also the antenna should not be taking-off when the mainframe is in the working-condition. The jammer shall be installed in the position with good-ventilation, and large-scale-things shall be avoided to ensure to the-shielding-effect. When use the jammer outdoors, preventing water shall be taken into consideration.

The GSM mobile-phones-used for testing of the jammer are: Samsung- GT-E1080T; Blackberry-7290; Motorolla, C118; Nokia-1100, 1661, 6300; Tecno-T570, T780; TV22i; and iPhonei9+. These-phones were fully-charged so as to avoid the risk of switching-off during the testing-process.

3. Results and Discussion

3.1. The simulated-circuit of mobile-phone-jammer

The simulated-circuit of mobile-phone-jammer is shown in Figure 4, while Figure 5 illustrates the Breadboard-Assembly of the jammer.

The jammer is powered by the 9V-battery D.C. The transistor Q1, capacitors C4 & C5 and resistor R1 constitute the RF-amplifier-circuit. This will amplify the signal generated by the tuned-circuit. The amplification-signal is given to the antenna through C6 capacitor, which removes the DC and allows only the AC signal to be transmitted. When the transistor Q1 is turned ON, the tuned-circuit at the collector will get turned ON. The tuned-circuit consists of capacitor C1 and inductor L1. This tuned-circuit will act as an oscillator with zero resistance. This-oscillator or tuned-circuit will produce the very-high-frequency with minimum-damping. The both inductor and capacitor of tuned-circuit will oscillate at its resonating frequency.

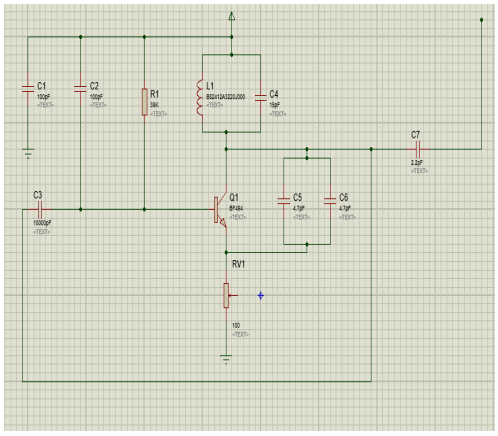

Figure 4: Jammer circuit diagram

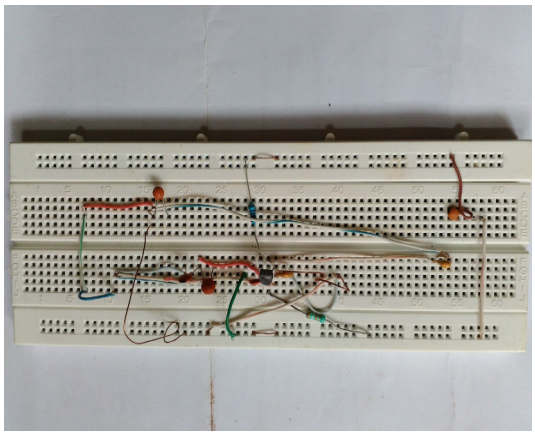

Figure 5: Breadboard-Assembly of the jammer

The tuned-circuit operation is as follows: When the circuit gets ON, the voltage is stored by the capacitor according to its capacity. The main-function of capacitor is to store electric energy. Once the capacitor is completely charged, it will allow the charge to flow through inductor, which is used to store magnetic-energy. When the current is flowing across the inductor, it will store the magnetic-energy by this voltage across the capacitor and will get decreased, at some point complete-magnetic-energy is stored by inductor and the charge or voltage across the capacitor will be zero. The magnetic-charge through the inductor will decreased and the current will charge the capacitor in opposite or reverse-polarity-manner. Again after some-period of time, capacitor will get completely- charged and magnetic-energy across the inductor will be completely zero. Again the capacitor will give charge to the inductor and becomes zero. After some time, inductor will give charge to capacitor and become zero and they will oscillate and generate the frequency. This circle run up to the internal-resistance is generated and oscillations will get stop. RF-amplifier feed is given through the capacitor C5 to the collector terminal before C6 for gain or like a boost-signal to the tuned-circuit-signal. The capacitors C2 and C3 are used for generating the noise for the frequency generated by the tuned-circuit. Capacitors C2 and C3 will generate the electronic-pulses in some random fashion, so-called modulating signals (noise). The feedback-back or boost given by the RF-amplifier-frequency generated by the tuned-circuit, the noise-signal generated by the capacitors C2 and C3 will be combined, amplified and transmitted to the air.

3.2 Testing of the jammer with corresponding- recommendations

The jammer was able to destroy a signal-receiving-condition for all-the-specified cell-phones (separately) and cut-off the connection between cell-phone and the base-station by producing intercepting-signal (noise), which can make jammer receive the same frequency with cell-phones. Satisfactory-jamming of a mobile-signal was confirmed by the blocking of the signals generated by mobile-phones in 2G and 3G-networks operated via Safaricom, Airtell, Orange, and YU local-service-providers, when the phone indicated "*no network*", thereby allowing no call to go through; with no-interference to other communication- means observed.

When the mobile-jammer was turned-off, however, the mobile-phones were not automatically-reestablished their communications and provided full-service, as expected. Therefore, to resume communication afterwards, the mobiles should be "re-set"- turned off and on-again again.

The range of jamming was also smaller than expected. This could be explained that mobile-jammer's-effect can vary-widely based on factors such as proximity to towers, indoor and outdoor-settings, presence of buildings and landscape, even temperature and humidity play a role. A higher-powered-RF-amp can be possibly-used to improve the range of the jammer and, therefore further-research is needed to ascertain this option.

This jamming-device only transmitted a jamming-signal and had poor-frequency-selectivity. This is a type "A" small-interference-jammer. Hence, in order to simultaneously-block signals with different-frequencies falling within the relevant-band, a chain of similar such-devices is required.

Calibration of the tuner-circuit to coincide with the jammed-frequency was also a concern. Also, it was difficult to block all-frequencies within the applicable-bandwidth. Obtaining components such as a VCO-chip proved difficult, as well as the transistor BF 494 was not available in the Kenyan-market; hence an alternative BC 548 was used which, probably, never provided the desired results.

The tuner-circuit should be better-calibrated to make it more-precise. This will also assist in blocking frequencies within the applicable-frequency-band.

After blocking GSM 900, DCS (Digital Cellular Systems) 1800, PSC (Personal Communications Services) 1900 and WCDMA 2100 MHZ the next target is blocking of 4G system that is 2400 MHZ. To prevent over-jamming, proper RF site engineering and extensive testing will be required.

Although the law (in some-counties) clearly prohibits using a device to actively disrupt a cell-phone

signal, there are no rules against passive cell-phone blocking. Many-Electronics-design-companies are now working on devices that control a cell-phone, but do not "jam the signal", so called" hybrid systems". In our busy-life most of people do use their mobile-phone while driving, which arise accidental-possibility, thus in future to reduce accidents the jamming system will operate whenever the driver turns on the ignition. The jamming-device receives radiation emitted by the phone and also will be able to tell whether the mobile-phone is being used by the driver or the passenger.

3.3. Potential Applications of the Cell Phone- Jammer

Police can block phone-calls during a drug-raid, so the suspects will be unable to communicate; Cell-phone-jammer can be used in areas where radio-transmissions are dangerous (areas with a potentially-explosive-atmosphere), such as chemical-storage-facilities, fertilizer-factories, petrol-stations or grain-elevators; Corporations can use jammers to stop corporate-espionage by blocking voice-transmissions and photo-transmissions from camera-phones. They can also be used in the areas like schools or academic areas, exam centers, medical facilities, public libraries, governmental-offices and high-security-areas like prisons, courts, scientific-research-laboratories and military-facilities among others. Jammers could offer an impressive-array of applications, indeed. But in practice, every device has its advantages and its limitations. As such, the legitimacy-spectrum of mobile-jammers must be discussed, at this-juncture, to give a full-picture.

3.4. Cell-Phone-Jamming Legal-Issues

The review-recorded-below do not claim to be fully-comprehensive-account of every-instance associated with the Legal-Issues related to RF-signals-jamming, however, the assessment does give a fairly-good-picture of the order of magnitude 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.

Cell-phone-jammers are illegal in most-countries, except to the military, law-enforcement and certain-governmental- agencies (ACA, 2003), as it is considered a "Property Theft" because a private-service-provider-company has purchased the rights to the radio-spectrum, and jamming the spectrum is a kind of stealing the property the company has purchased. It also represents a "Safety Hazard" because jamming blocks all the calls in the area, not just the illegal or annoying ones. Jamming a signal could block the emergency-calls, where there is a life and death situation. In addition, there could be some innovative misuse or even abuse of the mobile-phone-jamming-technology, for example, there has been an extensive-recent-chitchat on Twitter, that 5-star-hotel-chains installed mobile-phone-jammers to block guests' cell-phone-usage and force them to use in-room-phones at much-higher-rates (*personal experience*).

According to the ACA's Declaration Prohibiting mobile-phone-jammers (2003), currently, the most-serious and severe-legal-elimination of mobile-phone-jammers is in Australia, where, for example Section 189 of the Act makes it an offence to operate or supply, or possess for the purposes of operation or supply, a prohibited device, without reasonable excuse. Section 189 also details the penalties that apply if a person is found guilty: if the offender is an individual – imprisonment for two years; or otherwise – 1,500 penalty units (currently $165,000).

The reasons for the prohibition included: mobile-phone-jammers cause deliberate-interference to licensed-services and may cause interference to other-services operating in adjacent-spectrum-bands; All mobile-phones being used within a radius of up to four kilometers from the jamming-device could be 'jammed'; Concern that radiation-levels of high-powered-devices may result in human-exposure to levels of EMR, that exceed the maximum permitted under Australian-health-exposure-standards. This has implications for public-health and safety, especially in confined areas; Jamming would be likely, among other things, to substantially interfere with, or disrupt or disturb public-mobile-phone-services and have serious-adverse-consequences for public-mobile-phone-users by jeopardizing the quality and extent of carrier-services, preventing access to emergency-services and causing inconvenience to or loss of business for mobile-phone-users.

Other services likely to be affected by jammers: Examples of the types of radio-communications services operating in bands near those used by mobile-phones and potentially-affected by mobile-phone-jammers are: trunked-land-mobile-systems; fixed point-to-point links which carry anything from data to multi-channel voice communications; sound-outside-broadcast and studio-to-transmitter links; cordless-telephones; interference with electromagnetic- wave sensitive-devices such as life-support-equipment in hospitals (such as the apnea-monitor) and those in airplanes, and the large-number of devices authorized to operate under ACA-class-licenses (such as garage-door-openers and wireless LANs), emergency organizations (such as poison-information-centres and other-medical-services) or to the normal-phone-numbers for police, fire and ambulance. Mobile-phones are increasingly being used to request emergency-assistance from the police, fire or ambulance services in life-threatening or time-critical situations, for example during 2002-03, 29% (or 1,128,339) of the 3,953,564 genuine-calls to emergency-call-service originated from mobile-phones. There is some-evidence of a potential for mobile-phone-jammers to cause mobile phones to "lock up" and to remain-so after leaving the

jammed-area until the phone is "reset" (e.g. by turning-it-off and on-again). The user may be unaware that this has occurred and of the need to reset the phone (ACA, 2003).

Other-countries are dealing with the issue of whether mobile-phone-jamming should be allowed. There have been a number of positions taken by these countries; such as in United Kingdom (UK), Ireland, United States of America (USA), and Europe it is legally-forbidden. Canada: With respect to the use of jamming-devices in connection with federal-security and law-enforcement-functions for national-security-purposes, an alternative-authorization-process is, currently, under review. In Jamaica mobile-phone-jammers are used (with specified-restrictions) in prisons. There is, however, a media-report which suggests that legitimate-services outside the prison boundaries are affected. It has also been reported that universities in Italy have adopted the jamming-technology to prevent overwhelming-cheating, as the students were openly-taking photos of tests with their camera-phones and sending them to classmates (ACA, 2003).

From the above it can be ironically-perceived, that cell-phone-jamming-technology is, simply, an illegal-technology, which causes more-problems than it solves. In the local-context, however, Safaricom Company (the largest-mobile-service-provider in Kenya) of Vodafone group and Kenya-Prisons-Services recently announced (after several-pilot-studies) that they *will* install phone-jamming-equipment in all the major-prisons (CCK, 2014). This was termed as a response to the runaway-crime involving mobile-phones that is perpetuated by prisoners.

The strategy of jamming-mobile-phone-signals in prison compounds is a logical-technical-response. By creating islands of non-connectivity in these-jails, it is possible to mitigate the economic and social-risk posed by these incarcerated-criminals. CellAntenna states that jammers provide the-best and most-economical-way to prevent cell- phone use in prisons, require very-little-staff-time, and that the cost of the system depends on a number of factors such as the size and shape of prison, the area to be covered, and incoming tower signal levels (One News, 2007). Cell-phones, especially smart-phones, enable prison inmates' access internet and social-media-sites as well as receiving and sending short-messages, and videos which poses challenges to public-safety and rehabilitation (Norris, 2016). According to survey on inappropriate use and possession of mobile-phones in prisons of Kenya by Ochola (2015), 34% of inmates reported to have owned mobile-phones at one-given-time, 100% of the respondents agreed to have used mobile-phones and 78% have paid to acquire mobile-phone-usage from those inmates owning mobile-phones. On mobile phone usage different-reasons emerged: Criminal acts (swindling the public, threatening potential-witnesses and extortion, Maintaining contacts with family, Private-communication with minimal-oversight by authorities, Facilitation of escapes and Arrangement and co-ordination of contraband supply among others). Statistics from Safaricom indicate that most of the phone-related-fraud-cases originate from prisons; with Kamiti- prison taking the lead with about 1,500 fraudulent SMS and calls during one month only, which translates to 65 % of the total-incidents during the month. Other than Kamiti the practice is also ripe in other-prisons across the country including, Nakuru, Meru, Kibos and Shimola Tewa. Some-jailbirds arrange for their friends to throw mobile- phones across the wall of the prison after packing them in plastic-bags, which is considered as contraband. In another instance, a prisoner staged a 'nude protest' after the jail-authorities examined him following suspicion that he was hiding a mobile SIM card in the private-areas of his-body. Also, the jammers at the Kannur central prison (one of the pilot-projects) were recently switched off after the nearby residents seriously-complained that it was affecting their mobile-communication. No need to say that this delighted the Kannur prisoners.

4. Conclusion and overall recommendation

The aim of the project which was to build a simple-mobile-phone-jammer is achieved. Jamming-technique is potentially very-useful to disable cell-phone in a particular-range, but it should-not affect the other base station transmission-systems. Mobile-jammer can be used in any-location (subject to particular legal-restrictions), but, practically, in places where a mobile-phone-use would-be, on the whole, harmful, disruptive, and even dangerous, like in prisons. Overall-recommendation is that, further and more deeper-research is needed to produce more-sophisticated and better-jamming-devices, as to not affect the other base station transmission systems.

5. Acknowledgements

The authors would like to acknowledge the technical-staff of the Electrical Laboratory of ECE, SOE for providing necessary-facilities for this study, and to Morris Mwirigi and Andrew Macharia for the valuable-assistance in the conducting of the experiments and validation of the system.

References

Akaiwa, Y. (2008) Introduction to Digital Mobile Communication, 2nd Edition. ISBN: 978-1-119-04110-8 [Online] Available: http://eu.wiley.com/WileyCDA/WileyTitle/productCd-1119041104.html (June 12, 2016).

ACA (2003) Australian Communication Authority Report: Mobile Phone Jammers. [Online] Available: jamsrep.pdf (June 6, 2016).

Campbell, S. & Park, Y. (2008). Social implications of mobile telephony: The rise of personal communication society. Sociology Compass, 2(2), 371-387.

Cohen, J. & Graham, J. (2003). A revised economic analysis of restrictions on the use of cell phones while driving. Risk Analysis, 23(1), 5-17.

CCK (2015) Communication Commission of Kenya – Annual Report 2014/2015. [Online] Available:http://www.cck.go.ke/html/annual_reports.asp (May 22, 2016).

Daily Nation (2014) Most teens use phones for calls - Daily Nation , Jul 8, 2014. [Online] Available: www.commonsensemedia.org/blog/cheating-goes-hi-tech. (June 1, 2016).

Fielden, K., & Malcolm, P. (2008). Towards a deeper understanding of cell phones in schools: Aligning school policy. International Journal of Mobile Learning and Organization 2(3), 216-236.

Gralla, P. (2002). How wireless works. Indianapolis, IN: QUE.

ITU (2009). ITU Report for 2009: Kenya poised for huge growth in mobile services. International Telecommunications Union.

Gopal, A. (2013) Mobile Signal Jammer Using Arduino. Project-report for the degree of Bachelor of technology, department of electronics and communication engineering, Gokaraju Rangaraju institute of engineering and technology (Affiliated to Jawaharlal Nehru Technological University)

Ling, D. (1997). Mobile telephones and the disturbance of the public sphere. [Online] Available:http://www.academia.edu/2933684/Mobile_telephones_and_the_disturbance(April 17, 2016).

Mahato, S. and Vimala, C. (2015) Cellular Signals Jamming System in 2G And 3G. International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, ISSN (Print): 2320 – 3765 ISSN. Miao, G; Zander, J.; K-W Sung, and Slimane, B. (2016) Fundamentals of Mobile Data Networks, Cambridge University Press, ISBN 1107143217.

MPCC (2003)Mobile & Personal Communications Committee of the Radio Advisory Board of Canada "Use of Jammer and Disabler Devices for blocking PCS, Cellular and Related Services". [Online] Available: http://www.rabc.ottawa.on.ca/e/Files/01pub3.pdf (May 27, 2016).

Nation (2016)"KCSE results of a record 5,000 cheats cancelled", Nation newspaper (Mar. 04, 2016)

Norris, A. (2016) Mobile Phone Detect & Deny technology for Prisons. [Online] Available: mobile-detect-deny-prisons.pdf (June 11, 2016).

Ochola, G. (2015). The effect of contraband smuggling on rehabilitation of inmates in Kenya: the case of Kamiti-maximum-prison. Master's thesis, Kenyatta University.

Prensky, M. (2001). Digital natives, digital immigrants Part 1. On the Horizon 9(5), 1-6.

Prensky, M. (2005). What can you learn from a cell phone? – Almost anything! Innovate, 1(5), 1-8.

Tata, M. (2015) Programming and customizing the PIC microcontroller: Third edition. McGraw-Hill Education Pvt. Ltd, 7 West Patel Nagar, New Delhi 11008.

Zorn,S.; Maser,M.; Goetz,A.; Rose, R. and Weigel, L. (2011) "A power saving jamming system for e-GSM900 and DCS1800 cellular phone networks for search & rescue applications, Published in:

Wireless Sensors and Sensor Networks (WiSNet), IEEE Topical Conference, 16-19 Jan. 2011, Page(s): 33 – 36, E-ISBN: 978-1-4244-8413-3, Print ISBN: 978-1-4244-8414-0