International Journal of Women in Technical Education and Employment
ISSN: 2811-1567. Volume 3 – Issue 1. July 2022
https://fpiwitedjournal.federalpolyilaro.edu.ng

Cellphone Network Jammer Circuit Using NE555 Timer

Olayiwola Joy Oluwabukola & Aliu Olaniyi Habib
Department of Computer Engineering, Federal Polytechnic, Ilaro, Ogun State, Nigeria.
oluwabukola.olayiwola@federalpolyilaro.edu.ng; olaniyi.aliu@federalpolyilaro.edu.ng

ARTICLE HISTORY

Received: July 5, 2022
Revised: July 18, 2022
Accepted: July 23,2022

Abstract

Cellphones have been a significant way of communication, but sometimes they are also utilized as an instrument to commit crimes thereby affecting the security of the community. Cell phone usage at gas stations and oil refineries is dangerous and terrorist organizations can also make use of cellphone for bomb detonation. Cellphone network jammer helps to solve this problem by disrupting the network in different ways to maximize its effectiveness. Cellphone jammers consist of 3 major parts: the radio frequency amplifier, the voltage-controlled oscillator, and the tuning circuit. The jammer design comprises capacitors, resistors, inductors, transistors and NE555 clock IC to interrupt signal (noise) and also amplifies the generated signal to the lead of 800 MHZ to 1.4 GHZ in other to equal the signal of the cellphone range by the base position. The program and the calculi command will be examined to achieve the intended design. The concept of implementation, if fabricated accordingly, shall breathe fit of interrupting the GSM 900 and GSM 1800 signals coincidentally. The cellphone jammer device efficiently blocks local phones in a given range and can be used in examination halls, conference rooms, and even courtrooms.

Keywords: *Cellphone, Jammer, Signal, NE555.*

Citation
Olayiwola, J. O. & Aliu, O. H. (2022). Cellphone Network Jammer Circuit Using NE555 Timer. *International Journal of Women in Technical Education and Employment,* 3(1), 164-171

Introduction

Communication is the invisible thread that binds and connects people. The digital era offers a never-before-available array of communication, engagement, and information-retrieval options at one's fingertips (Akaiwa, 2015). Cellphones have great advantages to the community, they are also utilized sometimes as an instrument to commit crimes thereby affecting the security of the community (Campbell & Park, 2008). Due to advancements in science and technology, cellphone monitoring, and observation replaced majorly all previous inspection techniques and sources of information globally. Furthermore, using a cellphone at a gas station or an oil depot puts one in danger of physical harm, as it might produce a fire or a burst, both of which have major effects.

Terrorists can remotely use cell phones to detonate bombs and carry out other criminal operations like enrolling children for ISIS and other terrorist organizations. Terrorists have progressed from suicide bombers to using cellphone detonation because almost all populous region globally has cell phone network coverage, making it simple to explode bombs from anywhere around the world (Muhamed *et al.*, 2017). In such situations, an RF-jammer might be extremely useful.

According to Cohen and Graham (2003), they observed the leading cause of collisions is failure to maintain attention, and some drivers converse on cell phones or send text messages while driving, putting themselves and other road users in danger. Another major concern is the illegal usage of cell phones by convicts.

Seminar and conference organizers have recently complained about having difficulty in urging

participants to switch off their cell phone devices when a section is ongoing leading to numerous posters addressing this issue on walls.

However, incidences of students cheating on tests are common and growing both locally and globally, some students use cell phones to cheat during tests and examinations (Ataro *et al.*, 2016; Sitati *et al.*, 2016). The findings show that there is a clear necessity for parents, schools, and leaders to address the importance of digital ethics and identify innovative strategies to combat the current issue of excessive cellphone use.

Mobile Jammers

In the early days, mobile jammers were utilized by the military services to contain attacks by attackers who plan to cause havoc by deploying remote bombs. Portable jammers, like other types of radio frequency interference, prevent portable cell network use by sending radio surges along with the coequal frequency that portable cell networks use (Mahapo and Vimala, 2015).

An attacker plants malicious wireless nodes in a wireless network to cause purposeful interference. A jammer's jamming effect is determined by the power of its radio transmitter, its position, and its effect on the network or targeted node.

A jammer can disrupt a network in a variety of ways to maximize its effectiveness. A jammer can be classified as either basic or advanced, depending on its functionality. The two main approaches are either the noise strategy, in which additional noise is inserted into receivers to prevent them from receiving the proper information from the receiving signal or the phased strategy, which involves changing the phase of signals to prevent receivers that are using the phase from receiving the signal in the correct phase (Umratkar *et al.*, 2019).

This causes an obstruction in the cell network devices which is enough to render the communication device unusable. Any portable phone within the signal coverage area of a portable jammer will infer "NO NETWORK" when the jammer is triggered. Signals are intercepted as if the portable cell phones were switched off. All portable cellphone devices will instantly rrestore connections and give a wealth of utility once the jammer is turned off.

The impact of portable jammers varies greatly considering elements like closeness to the tower, the quantity of structures, geography, as well as temperature and humidity, all play a role. The choice of a portable signal interfering device is based on the essential scale, which ranges from an individualized portable jammer that can be employed to ensure undisrupted council with the guests to an individualized mobile portable jammer for the place, to a truly high-power armed forces jammer to block larger area (Zorn, 2011). Places of worship, university lecture halls, libraries, performance halls, meeting rooms, banks, and other venues where silence is appreciated fall under this category.

The jammer's output power is usually expressed in Watts or sometimes in dBm. Cellphone jammers have a scope of ranges, covering a few meters to kilometers for both pocket devices and advanced versions (Gopal, 2013). Noise attack is the most common method employed in commercialized jammers.

Mobile Jamming and Disabler Techniques

Several strategies to prevent portable cell phones from being used in restricted places were discussed in the RABC Mobile & Personal Communications Committee (M&PCC) meeting on June 22, 1999, with the following five methods being utilized or being developed:

Type "A" Device (Jammers)

The goal of this method is to replace the cell network's operating frequency with a more energy-efficient frequency. These jamming methods are usually equipped with a variety of self-contained and self-operating oscillators that send out interrupting frequencies capable of overriding signals used by communicating cell phones, including those used by cellular systems' control hubs for cellular use. These

mobile phones will block all interaction with other cell devices in that domain from transceiving calls whenever they are operational in that domain. This type of equipment only emits a limiting signal with a low frequency, causing interference with a broader portion of the communicable service spectrum than it was designed to target (Mahato &Vimala, 2015). "There are two types," stated "Jim Mahan," a technologist. The first is brute force jamming, which simply truncates all signals on that frequency. The issue is that it's like overthrowing the airwaves, thereby it expands the designated into a common broadcast region. The other emits a modest amount of interference that may be contained within a single cell block. To keep a facility under control, a lot of little jamming pockets are required (Miao, 2016).

Type "B" Device (Intelligent Cellular Disablers):
It's also known as "Intelligent Cellular Disablers" because it doesn't use the driving mediums to generate a jamming frequency. Although the circuit is a sensor, it has the ability to transmit with the cellphone base station. Once the device senses the presence of a cell signal in a "silent" zone, the control software in the base station executes a restriction-based protocol to allow the call to be established.

Type "C" Device (Intelligent Beacon Disablers)
This sort of jammer is also called "Intelligent Beacon Disablers," because it does not put out an interrupting frequency through the handle media like the type "B" circuit. When the circuit is set aside in a certain "quiet" area, it acts as an "indicator," instructing any cooperating node to interrupt or stop its radio function. Because this must be constructed on a certain design pattern from cellular/PCS, such as Bluetooth, only nodes that are identical to the frequency received would pick up in the signal radius of the indicator. When the cellular device moves out from the indicator's signal region, it should be able to re-initialize its routine function.

Type "D" Device (Direct Receive & Transmit Jammers)

The circuit is similar to type "A," but it includes a receiving circuit to ensure that the frequency interrupting device is always receiving, and when it senses the presence of a cellphone in the "quiet" room, it automatically communicates with it before interrupting the cell phone by sending out an interrupting signal. This interrupting signal will be provided as long as the mobile phone maintains contact with the control station; otherwise, no interrupting signal will be sent. As a result, this circuit is free of electromagnetism pollution in the form of unprocessed energy output, as well as the signal spectrum of the type "A" circuit-Jammer and is minimally disruptive to neighboring signals.

Type E Device (Electromagnet Interference Shield - Passive Jamming):
The idea behind this design is to use the EMI override approach to convert an area into a Faraday cage. The Faraday cage selectively interrupts, or effectively inhibits, potentially all E.M.R from entering or exiting a cage, such as a predetermined confined space. Improvements in EMI technology, as well as well-known current products, can potentially be applied to the design of newly erected structures for the "silent conference" arena.

Materials and Methods

Methods

The design methodology comprises three main parts and when merged, the product of the device will work as a jamming device. These three major circuit parts are:

1. The Radio Frequency amplifier:

It amplifies the energy of the radio signal to an output power sufficient to interrupt a frequency.

2. The Voltage controlled oscillator:

It creates a wireless frequency that will disrupt the mobile cellular network.

3. The Tuning circuit:

International Journal of Women in Technical Education and Employment
ISSN: 2811-1567. Volume 3 – Issue 1. July 2022
https://fpiwitedjournal.federalpolyilaro.edu.ng

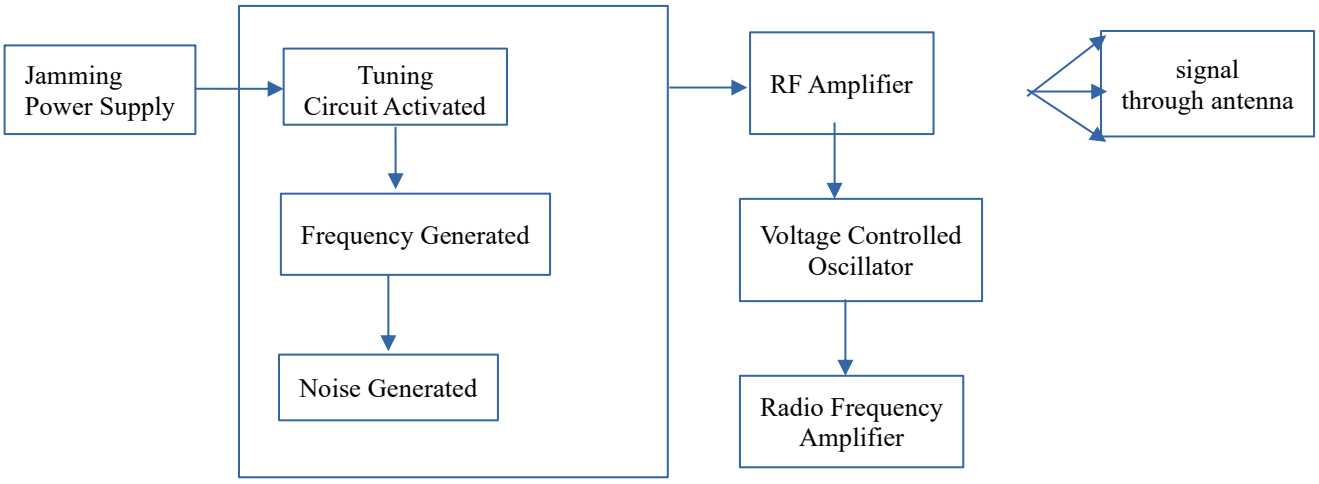

Figure 1: Cell phone jammer block diagram

This regulates the specified signal onto which the jamming device newscasts its frequency by outputting a certain volt to the oscillator circuit.

The cellphone jammer circuit was designed using proteus professional software. Figure 1 shows the block diagram of the cellphone jammer.

Jamming to Signal Ratio

When the interrupting frequency renders the interactive transmission signal useless, signal interruption is beneficial. When the inaccuracy ratio of the signal transfer cannot be equalized by fault correction in digital connections, the ability to utilise the transferred signal is jeopardized. A true signal interruption attack usually involves the energy of the interrupting circuit being plus or minus the energy of the receiving end's frequency (Tata, 2015).

The adaptable equation of the jamming-to-signal proportion is laid down as follows.

$$J/S = (PjGjrGrjR\,trLrBr) \;/\; (\,PtGtrGrtRj\,rLjBj) \quad \text{……. (i)}$$

where:

Pj = This indicates jammer power

Gjr = This indicates the antenna gain from the jammer to the receiver

Grj = This indicates the antenna gain from the receiver to the jammer

Rtr = This is the range between the comm of the transmitter and receiver

Lr = This is comm signal loss

Br = This is the comm receiver bandwidth

Pt = This indicates the transmitter power

Gtr = This is the antenna gain via receiver to the transmitter

Grt = This is antenna gain via receiver to the transmitter

Rjr = This is range in between the jammer circuit and a comm receiver

Lj = This is the jamming signal path loss

Bj = This is the jammer's bandwidth

The Jamming Frequency is calculated using the equation (ii):

$$F = 1/\,(2*pi*sqrt\,(L4*C6)) \quad \text{.....(ii)}$$

This parameter is truly significant in the system since the quantity of the product energy of the signal interrupting circuit relies on the demesne that's necessitated to interrupt. The design is initiated upon D = 10 measures for DCS 1800 band and D = 20 measures for GSM 900 band.

Materials

Table 1 lists the components utilized in the jammer, along with their relevant details while figure 2 shows the Cell Phone Signal Jammer Circuit Diagram.

A 9V battery D.C. is used to power the entire cell phone signal jammer. The CSW switch is used to turn on and off the cell phone jammer. The 555 clocks are used to create the frequency. A 1uf electrolytic capacitor delivers the output of the 555 clocks to the amplifier circuit. This capacitor blocks the D.C signal and allows the A.C signal to pass through, which is amplified by transistor Q1. A 4.7 pF capacitor is used to send the boosted signal back to the antenna.

.

Table 1: Components needed for the Cell Phone Signal Jammer

Component/Part Names	Component Value
NE555 Timer IC	
Transistor	NPN BF495
Capacitor (ceramic)	2pf
Capacitor (ceramic)	4.7pf
Capacitor (ceramic)	3.3pf
Capacitor (ceramic)	47pf
Variable / Trimmer (preset) Capacitor	35pf
Capacitor (electrolytic)	1uf 63V
Resistor	10k
Resistor	6.8k
Resistor	82k
Resistor	220 ohms
Resistor	5.6k
Air coil	24 turns x2
Switch button	1(SPST)
LED indicator	3mm (RED)
Battery	9V

International Journal of Women in Technical Education and Employment
ISSN: 2811-1567. Volume 3 – Issue 1. July 2022
https://fpiwitedjournal.federalpolyilaro.edu.ng

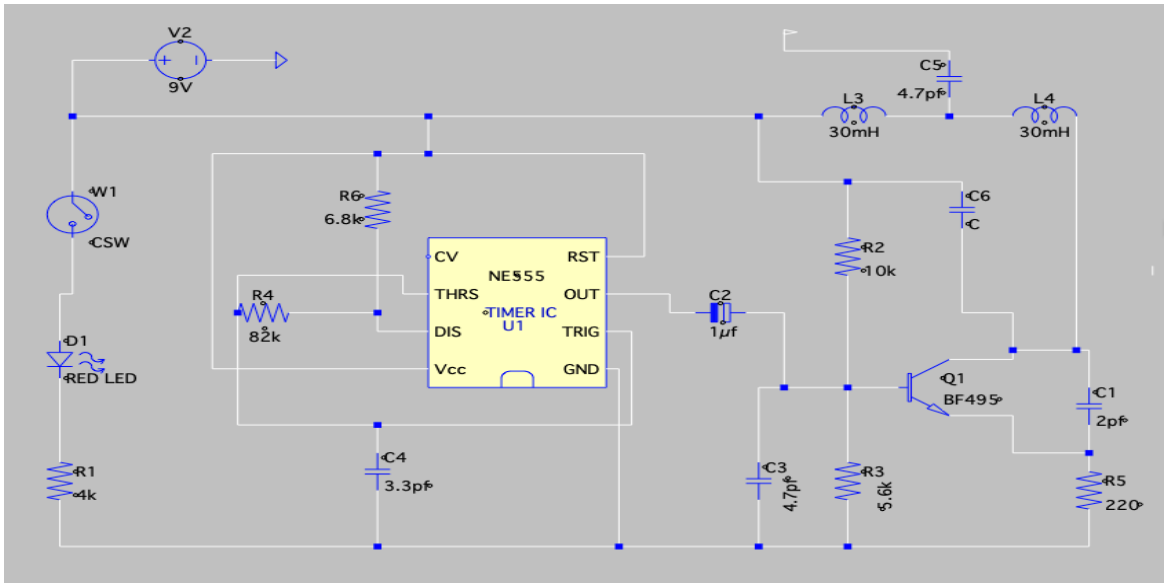

Figure 2: Cell Phone Signal Jammer Circuit Diagram

NE555 Timer

A 555timer circuit comprises two voltage comparators, one is a bistable flip-flop, a firing transistor, and a resistor separating the network. To understand the basic idea of the 555timer, we review it in a block form as shown below. The network of resistors separation is employed to place the comparator levels. Because all three resistors have the same value, the threshold comparator is internally represented by 2/3 of the supply voltage. A third of the supply voltage is used to represent the trigger comparator. These comparators' product is tied to a bistable flip-flop. The comparator changes state if the detector voltage falls below 1/3 of the supply voltage, and subsequently sets the flip-flop activating the output line to a high state. The capacitor voltage of these RC timer networks is normally maintained and monitored via the threshold line. Figure 3 shows NE555/556 timer functional circuit diagram.

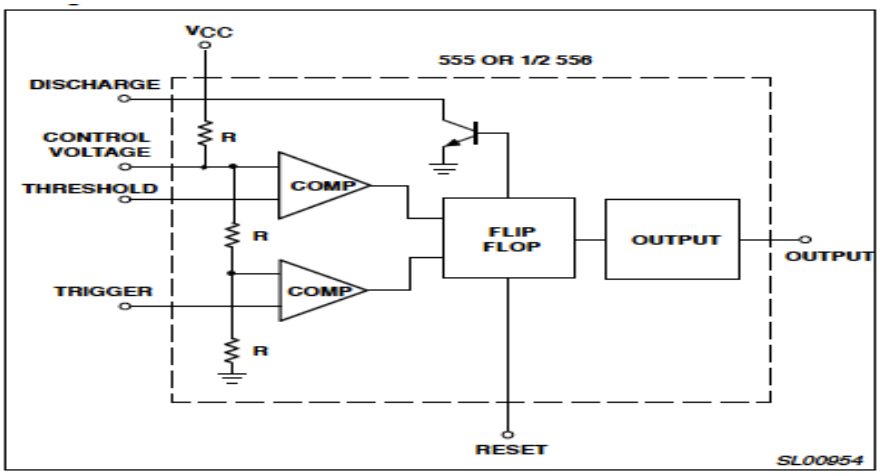

Figure 3: 555/556 timer functional diagram

International Journal of Women in Technical Education and Employment
ISSN: 2811-1567. Volume 3 – Issue 1. July 2022
https://fpiwitedjournal.federalpolyilaro.edu.ng

Major Components

The following major components are required: a power supply, circuitry, and an antenna. The jammer must also have an on/off switch as well as an LED that indicates whether it is on or off.

The circuitry of the cellphone jammer circuits, which consists of at least four major circuits that are linked together to give the output of that circuit to act as a jammer, was powered by a 9V power source. Voltage-controlled oscillator, tuning circuit, noise generator, and RF amplifier are among the components.

Results and Discussion

Simulated Cellphone Jammer Circuit

The oscilloscope reading of the cell jammer displays a single waveform with time on the horizontal axis and voltage on the vertical axis. The first graph in Figure 4 depicts a 9V provided voltage input, V (in), across the circuit. The second graph in Figure 4 displays the output voltage, V (out). It demonstrates the effect of the functional mobile phone jammer as a ramp waveform. The signal triggers the waveform with an increase of up to 3V at a time interval of 0.1 S once the jammer circuit is turned on, signaling the cellphone jammer is operational and capable of scrubbing the network signal. Figure 4 shows the jammer Simulation output.

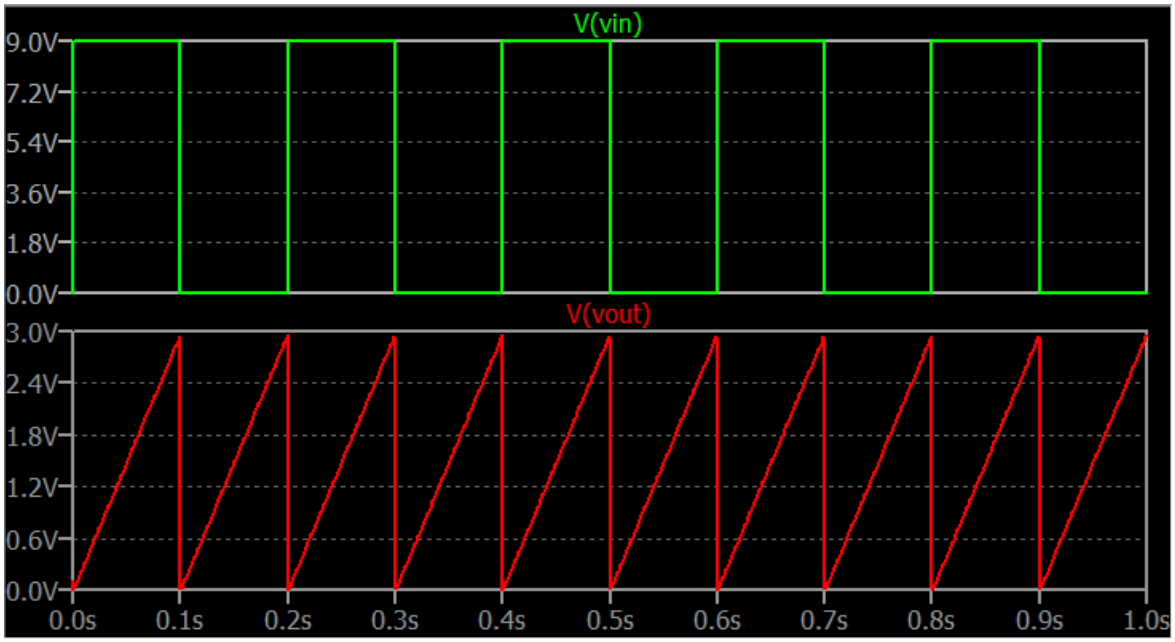

Figure 4: The jammer Simulation output

Conclusion

The mobile phone jammer device efficiently blocks the use of local phones, equivalent to providing humanity with endless protection. It's also adaptable for future additions. For data security, mobile device signal interruption can be used efficiently in all environments. The jammer setter must command all particular parameters appropriate for a mobile device, and the product energy must be more than the frequency available in the domain. Interrupting a local signal or preventing a mobile device from receiving or transmitting frequencies is a difficult task. The circuit must command an altitudinous level of pulsating generator with lucrative bandwidth to accomplish this task. The signal interruption circuit actively renders mobile devices ineffective in desired locations whenever it is used. These jamming circuits can be used in virtually any location ranging from exam halls, conference rooms, meeting rooms and even

courtrooms. It can also be used in hazardous chemical warehouses, oil refineries, and gas stations to prevent damaging contamination and explosions.

References

Akaiwa, Y. (2015). *Introduction to digital mobile communication*. John Wiley & Sons.

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

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

Gopal, A., Rahmaan, M. I. U., Reddy, P. N., & Reddy, Y. S. S. K. K. (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)*.

Madara, D. S., Ataro, E., and Sitati, S. (2016). Design and Testing of a Mobile-Phone-Jammer. Innovative Systems. *Design and Engineering*, 7(7), 7-18

Mahato, S. & Vimala, C. (2015). Cellular Signals Jamming System in 2G And 3G. *International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering*, 3, 242-247

Miao, G., Zander, J., Sung, K. W., & Slimane, B. (2016). *Fundamentals of Mobile Data Networks*, Cambridge University Press,

Muhamed, R., Milhajlo, M., & Zekirja, A. (2017). Terrorist Acts with Improvised Explosive Devices, The Threat to The Modern-World, The Example of The Islamic Republic of Afghanistan. *International Scientific Conference: Security Concepts and Policies-new Generation of Risks and Threats*, 25 - 41.

Sitati, S., Madara, D. S., & Ataro, E. (2016). Design of a Simple Cell-Phone Radio-Frequency Detector, *J. Inf. Eng. Appl.*, 6(7), 13–20.

Umratkar, P. Y., Chalfe, H. B., & Totade, S. K. (2019). Design and Performance of Mobile Phone Jammer. *International Journal of Engineering Technologies and Management Research*, 6(12), 1-5.

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: 33 – 36.