International Journal of Scientific Engineering and Applied Science (IJSEAS) – Volume-8, Issue-4, April 2022
ISSN: 2395-3470
www.ijseas.com

Implementation of a Low-cost Cellular Network Jammer

Segun Aina[1], Israel Akinpelu[1], Omolara Ogungbe[1], Niran Oluwaranti[1]

[1] Obafemi Awolowo University, Ile-Ife, Nigeria

Abstract

Cellular Network Jammer is a project designed to interfere with cellular communications in a restricted area. This study is aimed at designing a cellular network jammer with a level of performance with state-of-the-art jammers but at a lower cost. It employs Faraday's cage of conductive mesh jammer approach, in which an enclosure used to inhibit electromagnetic fields is constructed entirely of a conductive material (Aluminum). The project was tested using a Faraday's enclosure tester and the cellular network signals were detected to be blocked when the cellular device was fully covered in conductive material. This project's primary objective is to prevent mobile phone usage within its communication range without disrupting communication channels outside of its range, thereby providing a low-cost and dependable way for restricting mobile communication to the specified restricted areas exclusively.

Keywords: Low-cost, cellular network, signal jammer.

1. Introduction

Mobile phones' portability and convenience enable them to be carried in public places such as churches, lecture halls, and medical clinics. Because its convenience can be an annoyance in some areas and a security danger in others, there is a need to control their operations.

A cellular jammer is an electronic device that broadcasts signals at the same frequency as the Global System for Mobile Communication (GSM) system. When mobile phones in the area where the jammer is positioned are unable to work normally, the jamming is successful. Network Carriers operate on frequencies ranging from 900MHz to 1800MHz.

Mobile jammers were initially created for law enforcement and military usage to disrupt criminal and terrorist communications and thwart the use of certain remotely detonated devices. Civilian applications became obvious as public dissatisfaction grew over the increasing use of mobile phones in public settings and the reckless breach of privacy (Scourrias,1997). Many businesses that were initially hired to design mobile jammers for the government shifted their focus to selling these devices to private groups over time. As with other types of radio jamming, mobile jammers prevent people from using mobile phones by transmitting radio waves at the same frequencies as mobile phones (Jisrawi, 2006). This interferes with the communication between mobile phones and communications towers to the point that the phones are rendered inoperable.

2. Related Works

In the paper by P. Naresh *et al.* (2013), they implemented a prescheduled timer with a mobile jammer. The timer (activation and deactivation time schedules) was programmed with a Microcontroller. The jamming device broadcasts an RF signal in the frequency range reserved for cell phones that interferes with the signal, resulting in a "no network available" display on the cell phone screen. The activation

and deactivation time schedules were programmed using a real-time clock chip DS1307 to set the schedules. The real-time clock (RTC) chip is a widely used device that provides accurate time and date for many applications. The RTC chip present in the PC provides time components of hour, minute and second in addition to the date/calendar components of year, month and day. The RTC chip uses an internal battery that keeps the time and date even when the power is off. One of the most widely used RTC chips is the DS1307 from Dallas Semiconductor. The clock operates in either the 24-hour or 12-hour format with AM/PM indicator. The DS1307 has a built-in power sense circuit that detects power failures and automatically switches to the backup supply. Timekeeping operation continues while the part operates from the backup supply. The study successfully disrupted GSM services within a 5-7m range.

Uno *et al.* (2013) also designed and constructed a dual-band mobile jammer to sense phone signals and automatically deactivate the incoming or outgoing network signals. This jammer was designed to work at GSM 900mHz and GSM 1800mHz simultaneously and thus jammed the four well-known network carriers in Nigeria (MTN, GLO, Etisalat (now 9Mobile) and Zain (now Airtel).) as applied to lecture halls. It is evident from the results that the designed GSM jammer disabled mobile cell phone carriers in the GSM 900MHz -1800MHz bands.

Zakari *et al.* (2008) built a basic human size faraday cage. A 1-channel Electrocardiograph (ECG) circuit inclusive of notch filter was also built to test the effect of faraday cage, the outcome of the ECG signals was compared when placed inside the cage (i.e. inside the building), outside faraday cage (i.e. inside the building) and outside the main building. The study of the relationship between faraday cage and the effect on power line noise in ECG system was done and from the results it was seen that the faraday cage eliminated 50Hz power line noise in ECG signals.

Singh *et al.* (2017) paper proposed and aimed at designing a GSM Jammer. The project was mainly intended to prevent the usage of mobile phones in places inside its coverage without interfering with the communication channels outside its range, thus providing a cheap and reliable method for blocking mobile communication in the required restricted areas only. The circuits that made up the Jammer were the Tuning circuit, Voltage Controlled Oscillator (VCO), RF Amplifier and an Antenna. The simulation result and practical results were studied and were found to be approbatory equal. The Project was able to jam signals in between the frequencies of 890MHz to 960 MHz but not 1200MHz, due to the output power of the jammer being low. Further research proved if the Power input was increased the output power would have been stronger to jam frequency of up to 1200MHz.

Also, Jiswari (2014) designed a jammer that was able to block GSM 900 services. In this project, a GSM-900 Mobile Jammer was designed and built. The project was tested against the two GSM-900 Networks and proved successful with an average range of 10 m. It was advised that to improve the jammer, a more stable power supply should have been designed for robust operation of the device, as the power supply was not capable of delivering the needed current for the power amplifier and thus,

the reason for the actual coverage range of the device was not the same as designed for. Testing in different locations showed the jamming range's dependence on the signal strength. For instance, in low GSM coverage areas, the jamming range exceeds 20 m. In general, the jamming attack was protected by network signal power, and having a large power jamming device, the GSM network would be jammed for sure, and from this observation, it can be concluded that the protection against jamming attack in the GSM system was very weak and could not withstand the simplest jamming techniques. The mobile jammer's main disadvantage was the transmission of the jamming signal, which is prohibited by law in their countries. For instance, the fines for the offense could be very high. Despite the legal issues, high-power signal transmission may affect the operation of some critical devices, such as hearing impairment hardware solutions. These disadvantages will constrain the use of mobile jammers.

3. Theory

A cellular jammer is a device that intentionally interferes with communication between a mobile phone and its base station, effectively disabling all cell phones within the jamming radius (Wikipedia, 2021).
In the modern world, three distinct jamming tactics are used: spoofing, denial of service, and electromagnetic interference (EMI) shielding (also known as Faraday's cage of conductive mesh).
Spoofing is a technique in which the device coerces the mobile device into shutting down. This type is extremely difficult to deploy since the jamming device must first detect any mobile phone in a certain area before sending the signal to deactivate it. Certain variants of this method can detect the presence of a nearby mobile phone and deliver a message instructing the user to put the phone in silent mode (Intelligent Beacon Disablers).
In Denial of Service attacks, the device transmits a noise signal at the same operating frequency as the mobile phone in order to reduce the mobile's signal-to-noise ratio (SNR) to its minimal value, effectively jamming communications with the cell phone.
EMI shielding is a technique that employs EMI suppression to convert a room or enclosure into a Faraday cage. Although labor expensive, the Faraday cage effectively blocks or greatly attenuates practically all electromagnetic radiation entering or leaving the cage or target room. (Geetha, S. 2009)
Due to the sort of jamming technology employed in this project (EMI Shielding), a Faraday's cage is erected around a designated location, and upon arrival, all mobile phones display "NO NETWORK." As if the mobile phones were switched off, incoming calls are prevented. After leaving the area, all mobile phones will immediately reconnect and resume normal service (Callaghan 2021). The effect of a jammer varies significantly depending on its vicinity, the type of jamming technology used, the distance between cell towers, the interior and outdoor settings, the presence of buildings and scenery, and even temperature and humidity play a part (Zanger, 2006).

4. Materials and Method

Materials considered for implementation would be evaluated based on the following set of criteria;

- **Cost-Effectiveness:** The system is designed and implemented using available components at a reasonable cost.
- **Availability:** The Shielding Material used must be available and easily accessible.
- **Extensibility:** The system must be designed to add new capabilities without significant changes to the underlying architecture.
- **Compatibility:** The project target is to design a Cell Phone Jammer technique implemented in any facility.
- **The conductivity of the cage:** The larger the cage, the less the conductivity of the cage reduces.
- **Continuity of the conductive material:** The presence of a Faraday Cage via a lid or door creates the genuine possibility of such a break in continuity. If one side is discontinuous, even if it is conducting, the charge may not correctly redistribute, the canceling effect will be absent, and a non-zero field will exist within the cage. While connecting discontinuous edges with a wire can aid in low-frequency work, it is frequently insufficient for studies involving higher operating frequencies and speeds.

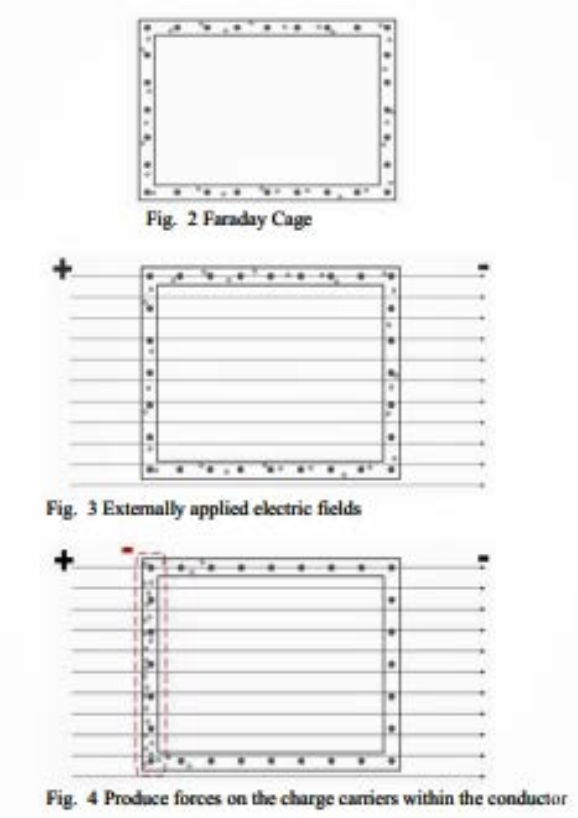
Materials needed for Faraday's Cage Construction are as follows,

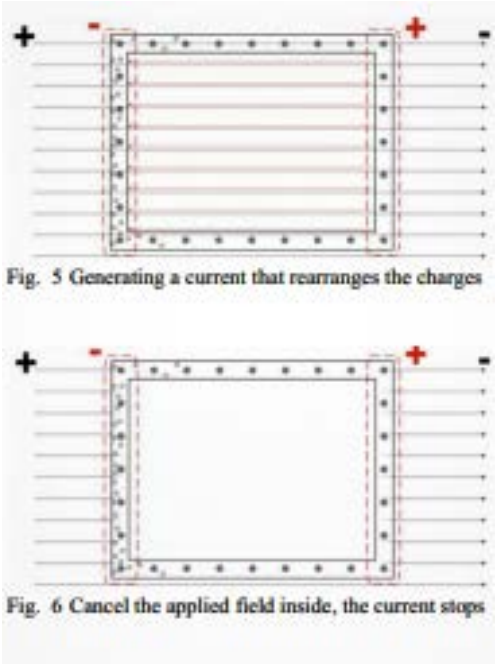
- A Box (can be wooden, metal, or cardboard)
- Conductive material (Aluminum foil was selected after evaluation)
- Adhesive tapes
- Cellular device

5. Experimental Setup

A Faraday cage model as shown in Figure 1, was built to prove the concept of EMI Shielding using the Faraday's cage concept. A Faraday cage is ideally understood as a close substitute for a hollow conductor as shown in Figure 2. to Figure 6. illustrating the working principles of Faraday's cage.

Figure 1. Faraday's cage Setup





Figures 2-6. Faraday's cage working principle

6. Methodology

A first attempt at demonstrating EMI shielding was done using two different boxes (One Unshielded and One Shielded with Aluminum foil have a Conductive Mesh) with cell phones placed inside them, as shown in figure 8. The shielded box as shown in figure 7, was initially lined with aluminum foil due to the effectiveness of the shielding effect that tends to increase with the conductivity of the shielding material, and with the conductivity of aluminum compared to copper and silver, which are high but not readily available. The enclosed phones were both dialed from another phone to see if they rang.

The Unshielded Phone rang successfully but the Shielded didn’t thus prove the cellular network was impaired by the Aluminum foil.

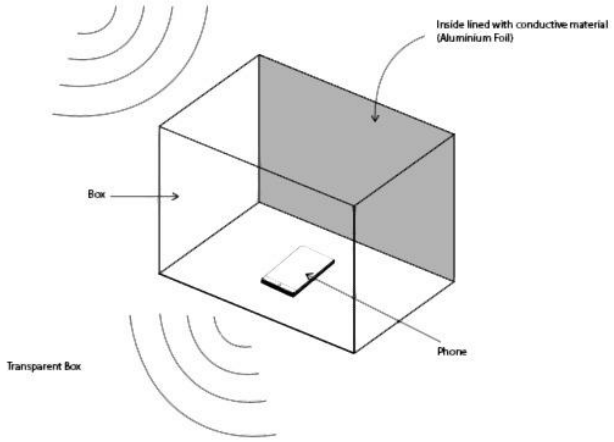


Figure 7. Faraday's cage Setup

Figure 8. Faraday's cage System design

Aluminum was selected as the shielding material due to its non-ferrous properties and high conductivity. Table 1 shows some common conductor materials and their levels of conductivity. Aluminum has nearly 60 percent conductivity compared with copper and Silver but these materials were not readily available for use (Chung,2020). Therefore, Aluminum was used. This metal needs precise attention to its galvanic corrosion and oxidation properties. The material will form into an oxide over time and has poor solderability on its own. Conductivity is determined by the types of atoms in a material (the number of protons in each atom's nucleus, determining its chemical identity) and how the atoms are linked together with one another.

Metals	**Conductivity (S/cm)**
Silver	6.8×10^5
Copper	6.4×10^5
Aluminum	4.0×10^5
Brass	1.7×10^5
Nickel	9.7×10^4

Metals	Conductivity (S/cm)
Steel	6.3×10^4
Stainless steel	1.8×10^4
Electroless Nickel	1.8×10^4
Graphite	5.0×10^2

Table 1. Conductivity of Materials

7. Result and Discussion

The concept of a Faraday cage has been proven using a model of a Faraday cage, consisting of a Box, a conductive mesh (Aluminum foil), a cellular phone. When the cell phone was placed inside the shielded box, it was observed that the signal strength started dropping drastically at 40 secs into the box and went to 0dB between 50 to 110 secs, as shown in Figure 9 below. While the cell phone was still in the box, the phones were dialed from other unshielded phones. It was observed that the mobile phones were unreachable. However, when the phone was brought out from the box, it regained connectivity, as shown in Figure 9, at 120 secs.

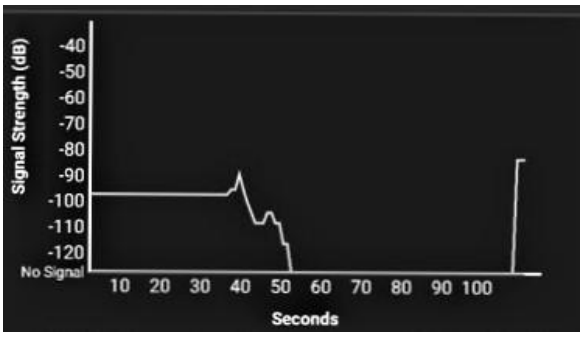


Figure 9: Signal graph

Readings on signal strength were taken via a Faraday enclosure tester application that measured the effect of the faraday's cage with respect to time. From the graph, it can be deduced that the signal strength of the device was -97dB before being put in the faraday enclosure. After 40 secs of reading the router signal strength, the device was put into the enclosure.10 secs into the faraday's cage and the

signal began to drop until it went to zero (0 dB) and "NO SIGNAL" was recorded. After 120 secs the phone was brought out and the signal was restored back to its original state.

8. Conclusion

This project's primary objective is to inhibit the use of mobile phones inside its coverage area without interfering with communication channels outside of its range, thereby providing a low-cost and dependable way for blocking mobile communications exclusively in specified, limited areas. The installation on a wide scale is quite labor demanding and static, i.e. it cannot be moved from location to location, but it is lawful in comparison to other types of Mobile Jammer that are prohibited or require a permit to use.

The Networks (MTN, 9MOBILE, AIRTEL, and GLO) were successfully jammed and communication was interrupted in the miniature Faraday's cage created for this purpose.

The Material used was aluminum foil as it is easily accessible and it effectively blocks signals into the Faraday's cage.

The limitation of the System included:

i. The System was not mobile and was only limited to the designed area.

ii. The material used was not efficient enough, thus leading to signal leakage.

References

[1] Ahmed Jisrawi (2006): "GSM 900 Mobile Jammer", undergrad project, Jordanian University of Science and Technology, Jordan.

[2] BYJUS (2021) - General Data Protection Regulation (GDPR) Guidelines. Retrieved March 31, 2022, from https://byjus.com/physics/electrostatic-shielding/

[3] Bbc.co.uk. (2011) - BBC History. "Michael Faraday (1791 – 1867)." Retrieved March 31, 2022, from http://www.bbc.co.uk/history/historic_figures/faraday_michael.shtml

[4] Chung, D. D. L. (2020). Materials for electromagnetic interference shielding. *Materials Chemistry and Physics*, *255*, 123587. DOI: 10.1016/j.matchemphys.2020.123587

[5] Wikipedia (2021) - Contributors to Wikimedia projects. *Mobile phone jammer*. Retrieved March 31, 2022, from https://en.wikipedia.org/wiki/Mobile_phone_jammer

[6] Geetha, S. (2009). *EMI shielding: Methods and materials A review*. Wiley Online Library. Retrieved March 31, 2022, from https://onlinelibrary.wiley.com/doi/full/10.1002/app.29812

[7] Murphy, T. (2010). Faraday cage. Magnet Lab Retrieved Feb 13, 2022, from http://www.magnet.fsu.edu/education/tutorials/tools/faradaycage.html

[8] O'Callaghan, J. (2021). *What is a Faraday cage?* Livescience.Com. Retrieved March 31, 2022, from https://www.livescience.com/what-is-a-faraday-cage

[9] Scourias, J. (1995). Overview of the global system for mobile communications. *University of Waterloo*, *4*. Citeseer.

[10] Uno, U. E., Okoye, P. F., & Charles, N. V. (2013). On The Physics of GSM Jammer and Its Application in Lecture Theaters. *Science Journal of Physics*, *2013*. DOI: 10.7237/sjp/144

[11] Wikipedia (2021) Wikipedia contributors. *Electromagnetic interference*. Retrieved March 31, 2022, from https://en.wikipedia.org/wiki/Electromagnetic_interference

[12] Zanger, Henry (2006): Semiconductor device and circuit, 3rd edition, McGraw-Hills Company, Singapore. http//www. Mobile and personal communications committee of the radio advisory board of canada .com: Use of Jammer and Disabler devices for blocking PCS, Cellular & Related Services.

[13] Zakari, N. A., Sudirman, R., & Jamaluddin, M. N. (2008). Electromagnetic interference effect from power line noise in electrocardiograph signal using faraday cage. 2008 IEEE 2nd International Power and Energy Conference. https://doi.org/10.1109/pecon.2008.4762559.

[14] P. Naresh, P. Raveendra Babu, K. Satyaswathi (2013). Mobile Phone Signal Jammer for GSM, CDMA with Pre-scheduled Time Duration using ARM7. International Journal of Science, Engineering and Technology Research (IJSETR).

[15] Saurabh Singh, KrishnaYadav, Rishabh Singh, Akash Soni, Harjeet Matharu and Pranay Rao, 2017. "Blocking of signal using signal jammer", International Journal of Current Research, 9, (11), 61326-61329.