DESIGN AND CONSTRUCTION OF MOBILE PHONE JAMMER USING EXTRINSIC NOISE

ABDULMAJEED MUHAMMAD KABIR

Department of Electrical and Electronics Engineering, Faculty of Engineering, Osun State University, Osogbo, Nigeria.

1.0 INTRODUCTION

A mobile phone jammer prevents communication with a mobile station or user equipment by transmitting an interference signal at the same frequency of communication between a mobile station and a base transceiver station. This project employs a system known as "active denial of service jamming" whereby a noisy interference signal is constantly radiated into space over a target frequency band and at a desired power level to cover a defined area. This jammer jams the downlink frequencies of the global mobile communication band - GSM 900 MHz and the digital cellular band - DCS 1800 MHz using noise extracted from the environment. This jammer works dual-band and jams three well-known carriers in Nigeria (MTN, AIRTEL and ETISALAT). The operational block of the jamming system is divided into two sections: Intermediate frequency (IF) section and the Radio frequency transmitter module (RFT). The IF section comprises a Noise circuit which extracts noise from the environment by the use of a microphone, this noise is mixed with a tuning (ramp) signal which tunes the radio frequency transmitter to cover certain frequencies. The RFT comprises an in-built voltage controlled oscillator, power amplifier and antenna connectors. An antenna radiates the jamming signal to space. Upon activation of the mobile jammer, all mobile phones will indicate "No-Network, SOS or Searching-For-Service**",** and all phones within the effective radius of the jammer are silenced. Incoming calls are blocked as if the mobile phone were off. When the Mobile jammer is turned off, all mobile phones will automatically re-establish communications and provide full service.

In conclusion, a jammer working on man-made (extrinsic) noise was constructed to interfere with mobile phones in places where mobile phone usage is disliked, offensive or forbidden.

2.0 RELEVANT CONCEPTS AND PRINCIPLES

The Broadcast Control Channel (BCCH) is one of the logical channels of the GSM system It continually broadcasts, on the downlink, information including base station identity, frequency

allocations, and frequency-hopping sequences. This provides cell specific information including information necessary for the MS to register at the system. One of the important sub-channels on the BCCH channel includes: Frequency correction channel (FCCH) which is used to allow an MS to accurately tune to a BS. It is required for the correct operation of radio system. This allows an MS to accurately tune to a BS. Synchronization channel (SCH), which is used to provide TDMA frame oriented synchronization data to a MS. This is also required for the correct operation of the mobile. Thus any destruction or disturbance in the broadcast control channel will render the mobile station incommunicado. Fig. 2 shows the GSM logical channels. Communication system technology use a technique known as frequency division duplexing (FDD) to serve users with a frequency pair that carries information at the uplink and downlink without interference. Fig. 1 shows the GSM FDD structures. A break in either uplink or downlink transmission results into failure of the communication link. This break can be as a result of weak signals due to proximity to the BTS, provided there is no handover. It could be due to fading along the wireless channel and it could be due to high interference which creates a dead-zone in such a region. The common factors that affect cellular reception include: strength and location of the cellular base station or tower, terrain and topology, weather and climatic conditions, structures, building material and construction methods. This project creates a dead-zone by utilizing noise signals and transmitting them so as to interfere with the wireless channel at a level that cannot be compensated by the cellular technology. The aim of this project is to achieve complete network disruption on GSM-900MHz and DCS-1800MHz downlink by employing extrinsic noise. The project is limited to operation at GSM-900 and DCS-1800 MHz cellular bands, with an effective jamming radius of approximately 10meters.

3.0 METHODOLOGY AND RESULTS

A noise generator is a circuit that produces electrical noise (random, non-deterministic signal). Noise generators are used to test signals for measuring noise figure, frequency response, and other parameters, it can also be used for the generation of random numbers. Several noise generation methods include: heated resistors, Zener diodes and gas discharge tubes. This project utilizes Zener diode noise method and also incorporates industrial noise which is sensed by Electret microphones with high sensitivity. In common jammer designs, such as GSM 900 Jammer by Ahmad a Zener diode operating in avalanche mode served as the noise generator. When Zener diodes are operated in reverse bias at a particular voltage level, they go into avalanche mode which results into a random current flow and hence a noisy

signal. In this project, Industrial (man-made) noise is mixed with such noise to create a signal with a higher noise signature. This industrial noise is tapped from the environment with the use of a high sensitivity microphone at -40 ± 3dB (0dB=1V/Pa,1KHz), placed in front of the jammer for better exposure to noise. With more microphones, a spatial diversity setting would be preferred. Although industrial noise is random and unpredictable, the Zener diode avalanche serves the noise requirement when jammer is used in an extremely silent environment.

The RF cellular transmitter module with 0.2W power amplifier simply turns a tuning voltage in the range 0-5V to a signal with frequency in the range 800-2100MHz. This covers the GSM and DCS.

A mobile phone might evade jamming due to the following reasons: strength and location of the cellular base station or tower, terrain and topology, weather and climatic conditions, structures, building material and construction methods, communication system technology, phone configuration, mobile network type, Act of God - Jammer Fault.

3.1 Test Equipment and Procedure

Digital oscilloscope capable of analyzing signals up to 30MHz was used to measure and analyze output waveforms at the intermediate frequency unit. Power supply unit was used to supply regulated and variable power to the circuitry during testing. A digital multimeter was used to measure resistance, capacitance, current and voltage levels. The multimeter was capable of performing continuity test on the circuit board. A blackberry phone (blackberry curve 9300) was used as the target mobile station for the jammer. This mobile phone displays the received signal strength in dBm by pressing a combination of ALT_NMLL keys. Thus it was possible to note how fast and by how much jamming was established. Livewire simulator package was used for some simulation tasks Each passive component was tested and value verified with respect to circuit diagram and available datasheet, this was done with the aid of the multimeter. Using laboratory breadboard, a prototype circuit was built and then transferred to a permanent circuit Vero-board. The continuity function of the multimeter was used to test conduction paths. The output of each circuit section was tested with the oscilloscope, clean probes were used and the time and voltage divisions were properly set to ensure the required output signal was visible. Noise circuit was tested while the laboratory fan was operational.

3.2 Results

The complete circuit of the jammer was switched ON and a blackberry mobile phone BB9300 was used to test the jamming effect. It was observed that the signal bars decreased and eventually went off. After

few seconds, the mobile phone signal appeared as either "searching for network". Range of the jammer was found to be around 10meters in indoor conditions. Fig. 7. shows a jammed blackberry phone

4.0 RELEVANT GRAPHICS

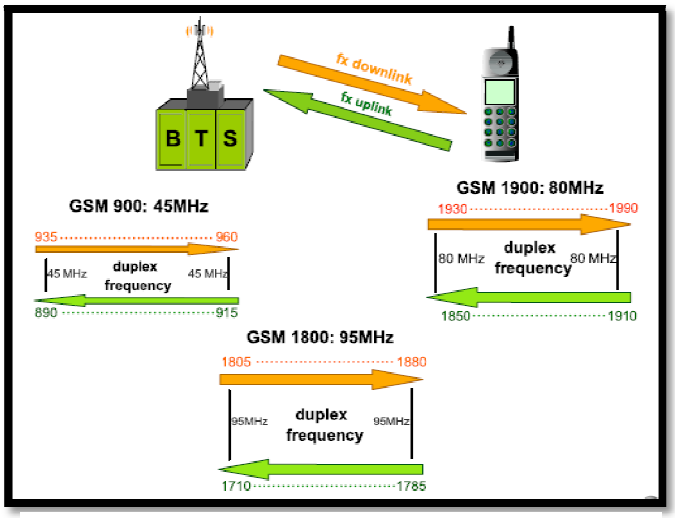

Fig.1. GSM FDD structure

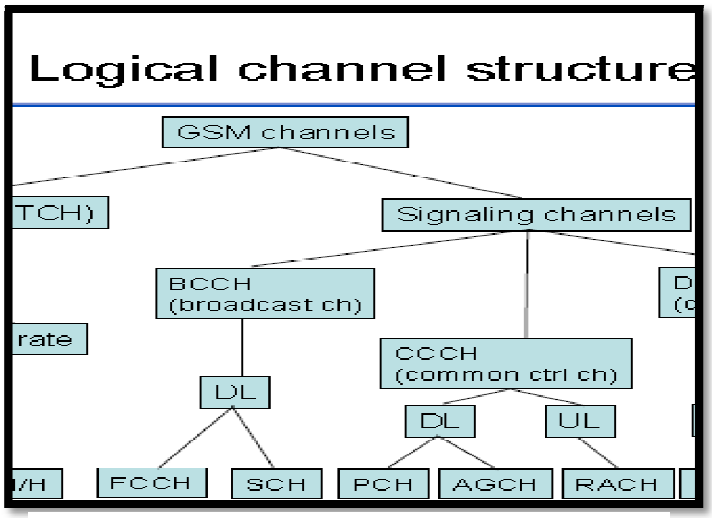

Fig.2. GSM Logical Channels

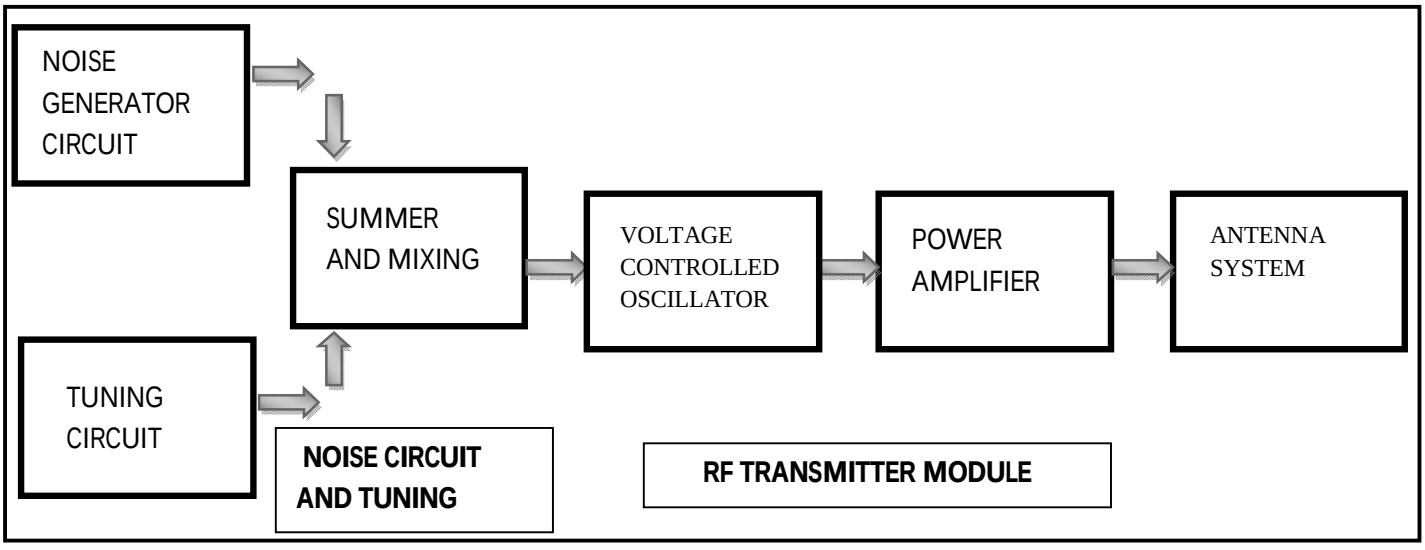

Fig. 3. Block diagram of Mobile phone jammer

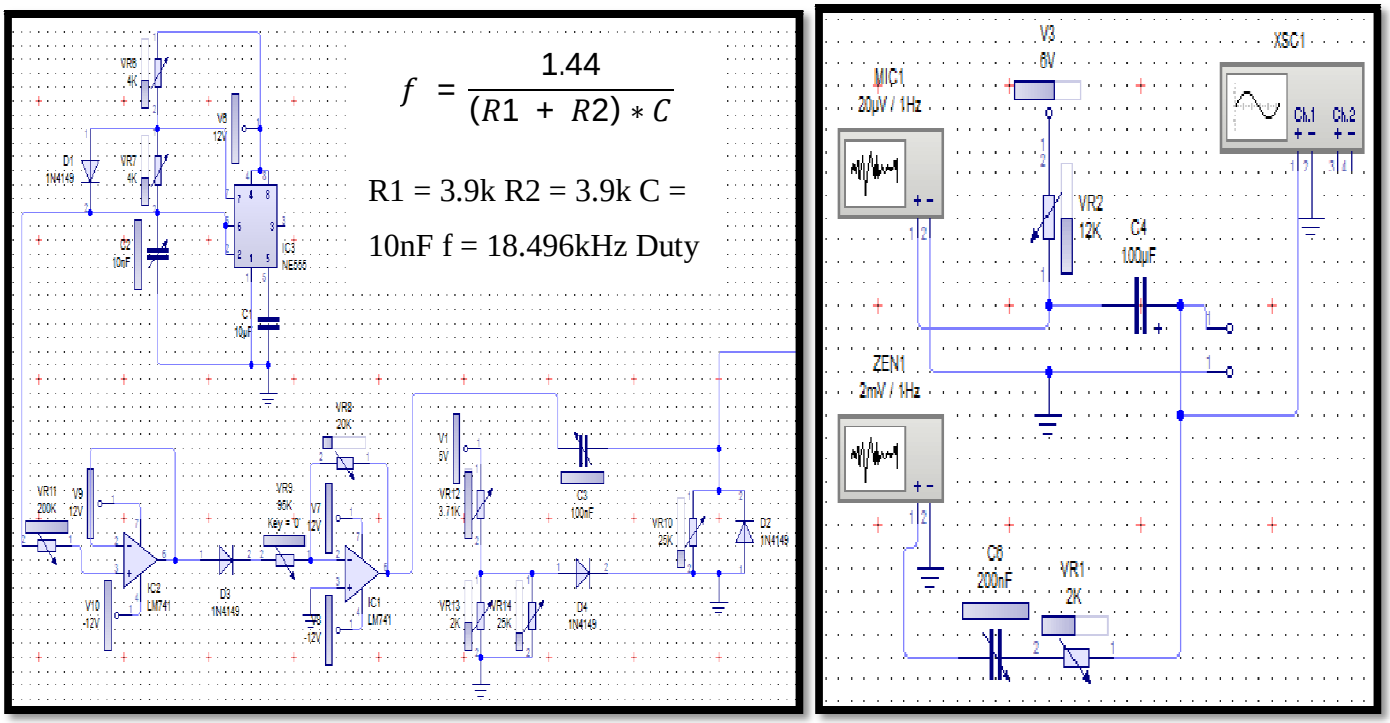

Fig. 4. Intermediate frequency and Noise circuit diagram

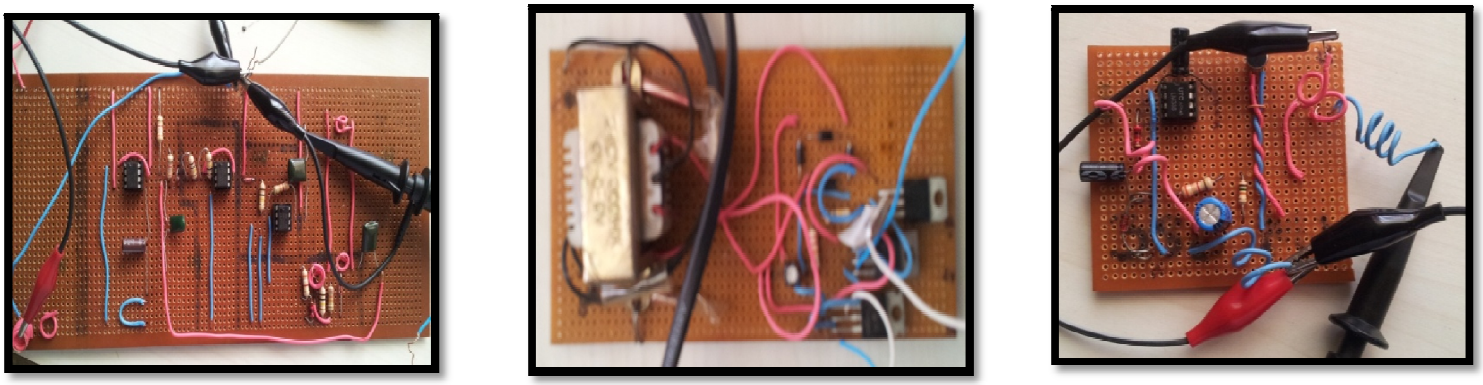

Fig. 5. Intermediate frequency, Power and Noise Circuits

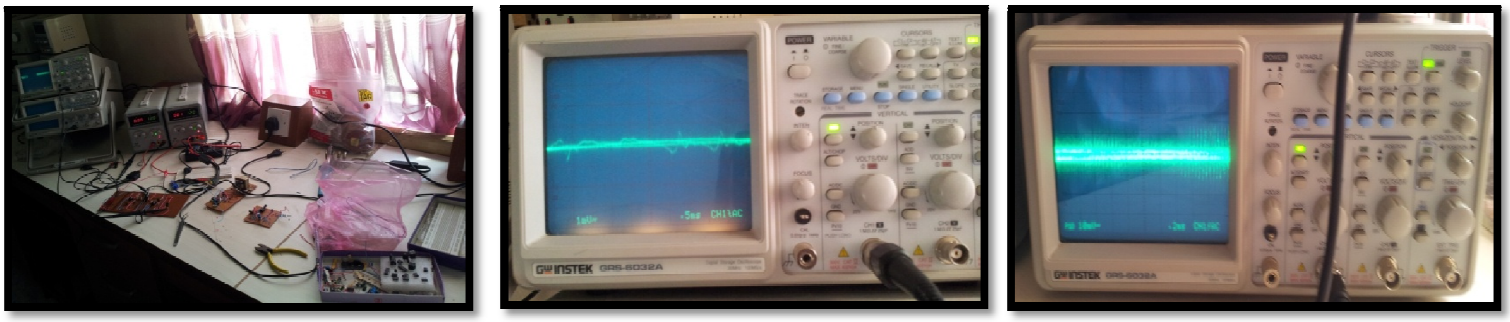

Fig. 6. Oscilloscope readings of Noise signals

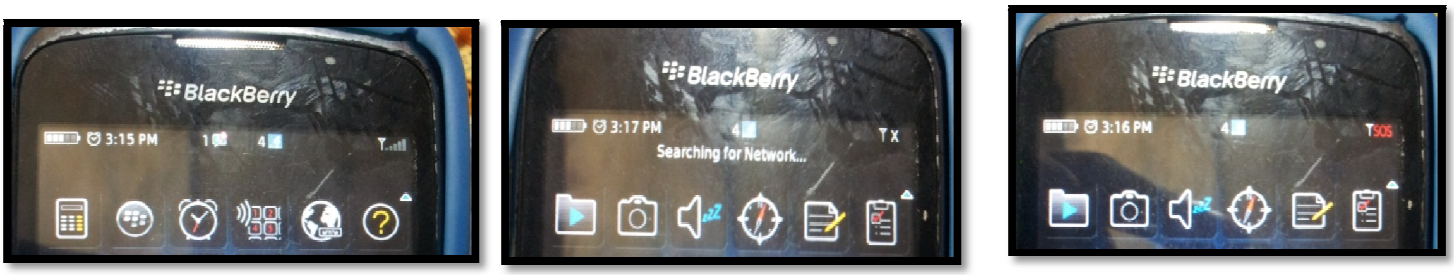

Fig. 7. Jammed Blackberry mobile phone

5.0 SIGNIFICANCE OF PROJECT TO NATIONAL NEEDS

The increased, incessant and alarming rate of the use of mobile phones during lecture hours can easily be pointed out as one of the factors affecting students of various institutions. The improvised smart techniques which students use in various forms of examination malpractices by which mobile phones are employed need to be curtailed. Likewise, communication between mobile stations can serve as a means of detonating improvised explosive devices (IEDs), a technique that is applied by both veteran and amateur terrorists, this is a major threat to life and property and is experienced worldwide. Since a mobile phone jammer thus proves a effective way of blocking the radio air-interface. Jammers are useful in the following: university lecture rooms, libraries, concert halls, meeting room, police stations, military, VIP protection, private users or secure rooms, convoy jammers, facility jamming, checkpoints, perimeter borders, anti-terror, prison solutions, board rooms, examination halls, auditoriums, mosques, churches, embassies, court rooms. In summary, the significance of a jammer is in three categories: security, education and discipline. From the work carried out on this project, it is feasible to tap noise from environment for use in engineering systems and possibly energy harvesting in the future. This is

due to the fact that noise is energy and is readily available like other sources of renewable energy. I envisage noise as a raw material in energy harvesting and in the future noise signature, tracking through Artificial Intelligence will improve security.

6.0 REFERENCES

- Mika Ståhlberg, Radio Jamming Attacks Against Two Popular Mobile Networks(2000)
- Radio Advisory Board of Canada, Mobile and Personal Communications Committee's meeting (1999).
- Jyri Hämäläinen, Cellular Network Planning and Optimization (2008).
- Kosola, Jyri: Communications COTS and EPM. MSc Thesis, The Royal Military College of Science, Department of Aerospace, Power and Sensors, Shrivenham (1998), 108p.
- Syed Ahmed, Shah S., Syed W., GSM Jammer (2006)
- Australian communications authority ACA Report, Mobile phone jammers (2003).
- Erik Jan van Lieshout et al, Interference by new-generation mobile phones on critical care medical equipment (2007).
- Mobile & Personal Communications Committee of the Radio Advisory Board of Canada, "Use of jammer and disabler Devices for blocking PCS,Cellular & Related Services" available at: http://www.rabc.ottawa.on.ca/e/Files/01pub3.pdf