JAMMING DESIGNING OF GSM AND CDMA SIGNAL

Joseph Bryan R[a], Nachrowie[a], Aries B. Setiawan*[a], Sanditiya Kristian S[a], Dinar Hana S. W[a].
[a]Electrical Engineering Department, University of Merdeka Malang
*Corressponding Author: aries@unmer.ac.id

Abstract

Jammer is a tool used to transmit signals at the same frequency, so the noise completely submerges the original signal in it. This system works when the device is placed in the jam's area which wants to be. Thus the device will disturb the transport of information from the sender to the recipient. This device is also useful on facing the war of electronic devices if it is developed in the military environment. The rate enhancement of mobile user can issue some problems at certain place, for insrance worship, lecture halls, libraries, concert halls, conference rooms, etc in daily life. Hence it need to be disabled as mobile phone rings will annoy those places. Jammer is used to interfere with GSM and CDMA operator signals by using square waves and triangular waves, then VCO combines them to produce the interference signals. Then RF transmitters will amplify it to jam the cell phone signals latter.

Keywords : Jammer, GSM, CDMA, Square Wave, Triangle Wave, VCO.

1. Introduction

1.1 Background

The development telecommunication's technology especially mobile phone has provided many benefits for human beings. However, if it is not used with proper time and place, it will harm the other side. Those places are, Hospitals, worship, etc. While the less appropiate time that is during a meeting and doing teaching learning.

Therefore, a Jammer system is developed to transmit signals at the same frequency, so that the signal captured by mobile phone will be interfered and it will disturb the communication system.

1.2 Research Question

Based on this background, the formulation of problems that arise in the designing and establishment of Jamming GSM and CDMA signals is: How to design a Jamming tool which can work and block the frequency on the phone with the allocation 900 - 1800 MHz for GSM and 800 - 1900 MHz for CDMA by using square and triangle wave which will be coupled VCO to be amplified on RF amplifier?

1.3 Reserach Purpose

The purpose of this research is able to develop the design of jammer device which can work and block the frequency on the phone with the allocation of 900 - 1800 MHz for GSM and 800 - 1900 MHz for CDMA by using square waves and triangles that will combine VCO to be amplified on the RF amplifier.

ISBN: 978-979-3220-41-3

2. Literature Review

2.1 GSM (*Global System for Mobile Communication*)

GSM is a digital cellular technology by utilizing microwaves. The delivery signal is divided a part of time, so that the signal information will reach the destination. In the beginning of its operation, GSM has anticipated the rapid number of users and the direction of service at each high area, so that the development direction of GSM technology is DCS or Digital Cellular System at 1800 MHz frequency allocation.

2.1.1 GSM Network Architecture

A GSM network is built from several functional components that have their own specific functions and interfaces, those Switching Sub System (SSS), Radio Sub System (RSS), and Operation and Maintenance Sub System (OMS).

Switching Sub System (SSS)

Switching Sub System or abbreviated SSS is a combination of interconnected devices to support the switching function of communication among each customers, customers with other networks, and customer databases. SSS consists of several parts, namely:

- MSC (Mobile Switching Center)
- HLR (Home Location Register)
- VLR (Visitor Location Register)
- AuC (Authentification)
- EIR (Equipment Identity Register)
- IWF (Inter Working Function)
- EC (Echo Canceller)

Radio Sub System (RSS)

Radio Sub System or abbreviated RSS is a hardware device that aims to support the function of communication systems, so there is a close relationship between SSS and RSS. RSS's equipment include:

- Mobile Station (MS)

MS is the equipment used by the users to access the mobile network. MS is divided into two parts, namely SIM (Subscriber Identity Module) and ME (Mobile Equipment) which refers to the physical telopon itself. A ME also has Transceiver (Tx) and Receiver (Rx).

- Base Station Sub System (BSS)

BSS is an important device which regulates Base Transceiver Station with Radio Controllter for customer traffic (voice traffic, signaling, data) up to core network or commonly called NSS (Network Sub System). BSS is divided into three parts, as below:

- **Base Station Controller (BSC)**

BSC serves as interfacing to MSC, Base Tranceiver Station (BTS), and Operation and Maintenance Subsystem (OMS), and it also controls base stations under its control, radio management, handover process, and BMS OMS functions adjusting.

ISBN: 978-979-3220-41-3

- **Base Transceiver Station (BTS)**

It can directly interact with MS through a radio interface which consist of Tx and Rx and performing physical layer management in the radio interface.

- **Transcending and Adaption Unit (TRAU)**

TRAU functions to encode speech (Speech transcoding) from BSC to MSC and vice versa, and also adjust the rate of voice data from 64 kbps out of MSC to 16 kbps to BSC for transmission channel efficiency.

Operation and Maintenance Subsystem (OMS)

The OMS is GSM network element that performs various purposes which is related with network operation and maintenance, such as monitors the functions of various network elements, performs interference management, network configuration, and performance.

2.1.2 GSM Modulation

The technique in GSM modulation is GMSK (Gaussian Minimum Shift Keying). This technique works by passing the data to be modulated via Gaussian Filter. The way to generate GSMK is by passing NRZ (non return-to-zero) data via Gaussian Filter which has an impulse response. This system releases the information signal contained in the carrier signal for GSMK, generally outputting a 900 MHz carrier signal.

2.2 CDMA (*Code Division Multiple Access*)

CDMA (Code Division Multiple Access) uses spread-spectrum technology to distribute information signals over a wide bandwidth of 1.25 MHz. CDMA is also a form of multiplexing (not a modulation scheme) and a shared access method that divides the channel by encoding data with a special code associated with each channel. CDMA technology is designed not to be sensitive towards interference, and some subscribers in one cell can access the frequency spectrum band together since they use certain coding techniques. There are two types of CDMA phones, without a card so that the call number must be programmed by the dispatcher and the CDMA phone with RUIM (Removal User Identification Module) or in GSM is known as the SIM card.

2.2.1 CDMA Components

Physical Components of CDMA consists of : User CDMA Mobile device in the form of mobile phone, computer, etc .; BTS; CDMA operators in charge of management traffic from the flow of information traffic; Dash Satellite as a link between sending signals from Earth to satellites; And Satellite as a liaison between remote and unreachable areas by BTS and earth transmitting stations.

In other hand the technical components of the spreading and despreading grooves on the CDMA system, namely: Data source which is a signal information to be sent and spreading code which is the process of expanding the information media by coding a signal information with a particular password at the same time and frequency.

ISBN: 978-979-3220-41-3

2.3 Square Wave Circuit

To generate a square wave in this circuit is used IC NE566 which is combined with resistor with capacitor.

2.4 Triangle Wave Circuit

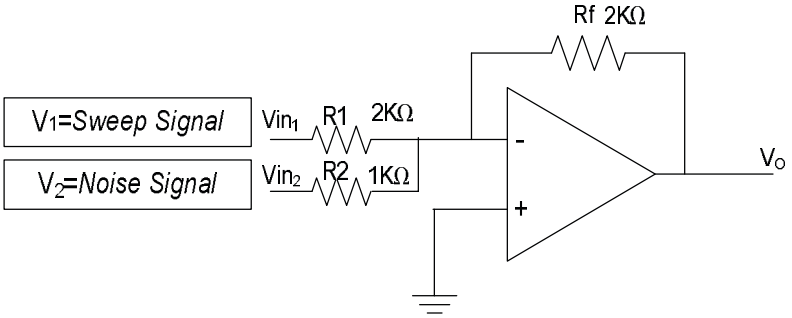
The triangle wave generator is an exponential shape which close the triangular shape, in order to near the linier, the capacitor C must be charged or discharged with a constant current. Therefore the Vcc changes linear (Subekti, 2012). Then the triangle waveform can generate by using NE556 IC circuit.

2.5 Noise Generator

Noise is defined as unwanted electrical signals with a broadband spectrum less than 200KHz that rides on the voltage or current of the electrical power system. Basically, the noise consists of unwanted distortions of signals, electrical power, where the signal can not be classified as harmonic or transient distortion. Noise will help for dismissing the jamming transmission, so the output signal looks like random noise. The noise generator circuit also consists of a standard zener diode with a little reverse current, a buffer transistor and an audio amplifier that serves as a band-pass filter and a signal amplifier. Noise generator has important function in the jamming system because it works to produce random electronic output at certain frequency to cut off the cell phone signal network (Subekti, 2012).

2.6 Mixer Circuit

The mixer circuit is an amplifier or summing circuit. The outlet waveform, Tringular Wave Generator, and Noise generator will be mixed and processed in the mixer before enter the VCO (Volt Control Oscillator) on the radio frequency section section.



Picture 2.1 Amplifier Circuit.
(Source : Ahmed Jisrawi, "GSM 900 Mobile Jammer", undergrad project, 2006)

In the above amplifier circuit is the summing amplifier, where the current (I) flowing through the parallel resistance Rf is equal to the number of currents passed by the series resistors R1 and R2 (Jiswari, 2006).

2.7 DC Offset Circuit

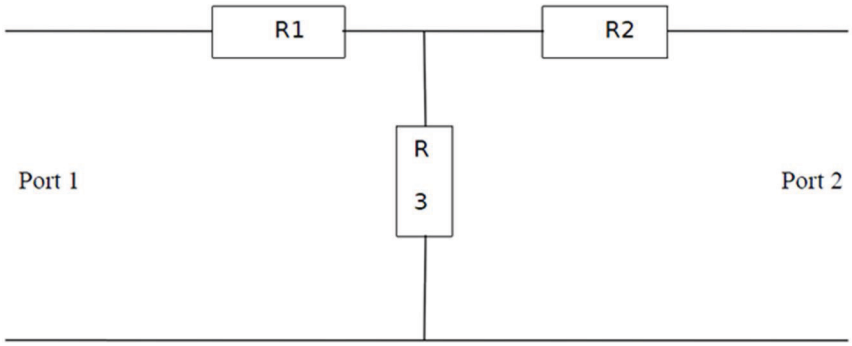
DC offset is a state of a DC current in an alternating electric power system which is caused by geomagnetic charge and the use of a single wave

ISBN: 978-979-3220-41-3

rectifier device. These components containt Clamper Diodes and potentiometers as control bias voltage.

2.8 Radio Frequency Section

Radio Frequency Section is the most important component circuit in the jammer system because the phone will interact with this component. RF section consists of VCO, RF Amplifier, and antenna. VCO is a circuit that produces an insulated output voltage. In the jammer system, the VCO part produces an RF signal that will jam mobile signal phone, as for strengthening the transmitter power of a transmitter used RF amplifier. The first amplifier is called the predriver, the next amplifier is called the driver, and the final amplifier is called the final. Here's a picture of the amplifier circuit.



Picture 2.2 T-Network Attenuator
(Source : Ahmed Jisrawi, "GSM 900 Mobile Jammer", undergrad project, 2006)

Before needing RF amplifier (1 - 5 dBm), used 4dB T-network attenuator as shown in figure.

3. System Designing

3.1 Designing Variable

In the design and manufacture of jamming tools, GSM and CDMA is focused for a radius of the wide range of tools with a distance of 1 - 21 meters. Some basic circuit that will be used is, power supply, circuit wave box, triangle wave circuit, mixer circuit, VCO, and RF amplifier.

3.2 Modeling Scheme

In this modeling scheme that is necessarily concerned in the experiment is the specification of jammer devices, and mobile phones that will be used in jammer tool.

Jammer Device Specification

- Frequency : 930 – 960/1805 – 1850 MHz (GSM) and 870 – 880/1975-1980 MHz
  (CDMA).

ISBN: 978-979-3220-41-3

- Radius : 20 meters
- Antenna : 4 external

Cell Phone Specification

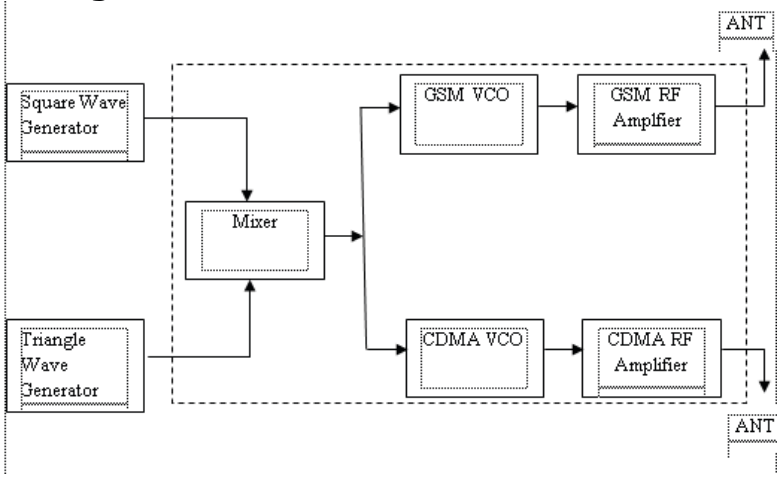
a. Mito 212

- Network : GSM 900/ 1800 MHz
- Color : Hitam
- Antenna : Fixed Internal
- Dimension :107 x 44.8 x 14.3 mm

b. ZTE C261

- Network : CDMA 1x 1900 MHz
- Color : Silver
- Antenna : Fixed Internal
- Dimension : 107 x 45 x 14,5 mm

3.3 Block Diagram



Picture 3.1 Block Diagram

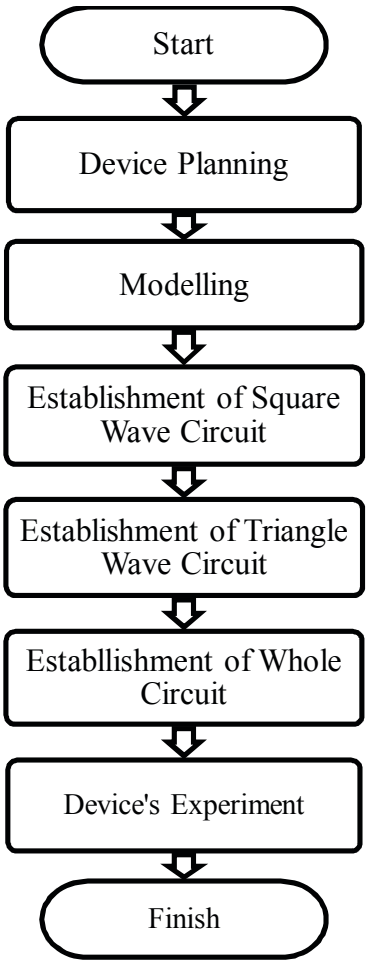
Based on the block diagram above, there is an intermediate frequency section consisting of square triangular wave generation, and GSM and CDMA module to emit jammig signals.

The second part, there is a radio drequency section consisting of VCO, RF amplifier, and antenna jamming where the mixer output goes to the VCO. There are two kinds of VCO, namely VCO GSM and VCO CDMA. Before transmitted through the antenna, the frequency signal is reinforced via a radio frequency amplifier. Then, the output RF amplifier circuit is connected to the antenna.

3.4 Flowchart Diagram

Here is a flowchart designing a jamming tool as below:

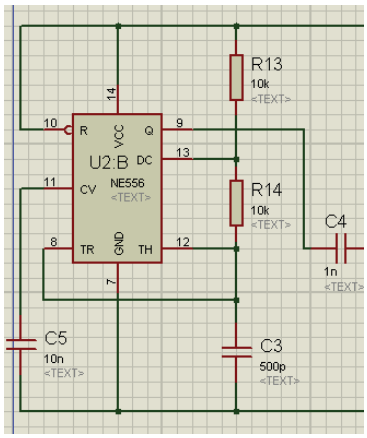
ISBN: 978-979-3220-41-3



Picture 3.2 Device Flowchart

3.5 Planning Square Wave Generator

There are two pieces of 10 kΩ of resistors, 1 nf, 10 nf, and 500 pf of capacitors, and Vcc of 5 V (DC). In the waveform generator circuit as shown in the figure.

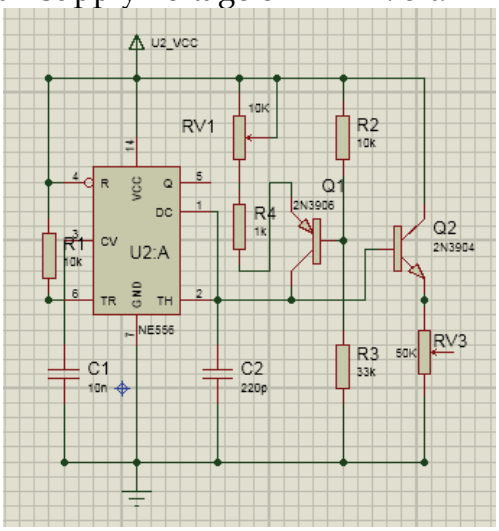


Picture 3.3 Square Wave Circuit
(source: support@innovativeelectronics.com)

ISBN: 978-979-3220-41-3

3.6 Planning Triangle Wave Generator

To get the triangle wave, it is planned an external circuit with RV1 and R1 of 10K **Ω,** R2 of 10K **Ω**, R3 of 33 K **Ω**, RV3 of 50 K **Ω**, C1 10 nf, C2 220 pf, and Vcc of 5 V. IC NE556 can supply voltage of 4 - 12 Volt.



Pictuer 3.4 Triangle Wave Circuit
(Source: support@innovativeelectronics.com)

3.7 VCO Modul and RF Amplifier

Output power generated power of 3 Watt and VCO 1900 - 1990 MHz for CDMA. While the output power of GSM 5 Watt and VCO 880 - 915.

3.8 Working Tool System

When the device is on, the NE556 IC will generate a triangle and square wave. Then they are mixed to be amplified through an RF amplifier and forwarded to the VCO where this process takes place inside the module. VCO will produce GSM and CDMA frequency oscillations. Furthermore, the frequency will be reinforced by the RF amplifier, then will be transmitted by Tx.

3.9 Experiment Planning

In this experimental planning used experimental steps that use several mobile operators, namely Mito 212, Esia One Touch 220C and ZTE C261. While opertor - operator to be used are:

- GSM Indosat (IM3), Telkomsel (As), XL, dan NTS Axis.
- CDMA Smart dan Esia.

4. RESEARCH RESULT

4.1 Analyzing Experiment Result

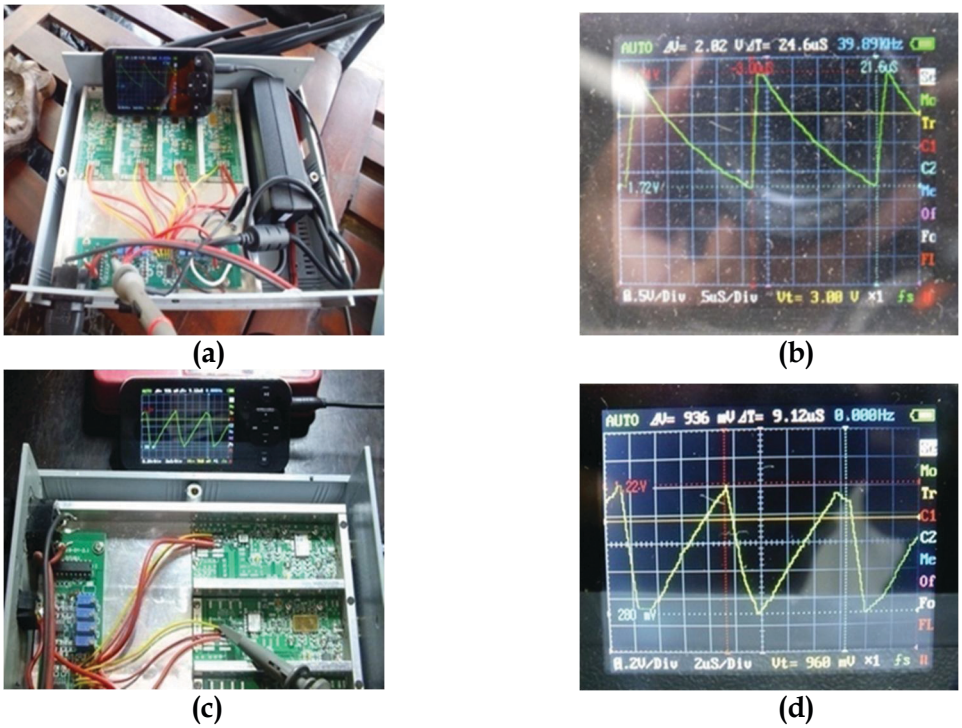
When the power button is on, the signal jamming process starts. After a while the cell phone signal gradually disappears and eventually nothing exists at all.

ISBN: 978-979-3220-41-3

4.2 Reseach Result

Measurement's Result of Jammer's Device by Using Oscilloscopes

This measurement is performed to determine the input and output signals of the square, triangle, and module waves. The results of the measurement



Picture 4.1 Measurement's Result of Triangle (a and b) and Square (c and d) Wave of Output Signal

In measurement of triangle wave input circuit is done on pin 9 IC NE556 (U2: B), while box wave input is done on pin 2 IC NE556 (U2: A), where the measurement of input signal can be seen in the pictures a and b.

Measurement of Output Signal in GSM and CDMA Module

The measurement result of GSM module in VCO + RF Amplifier module are:

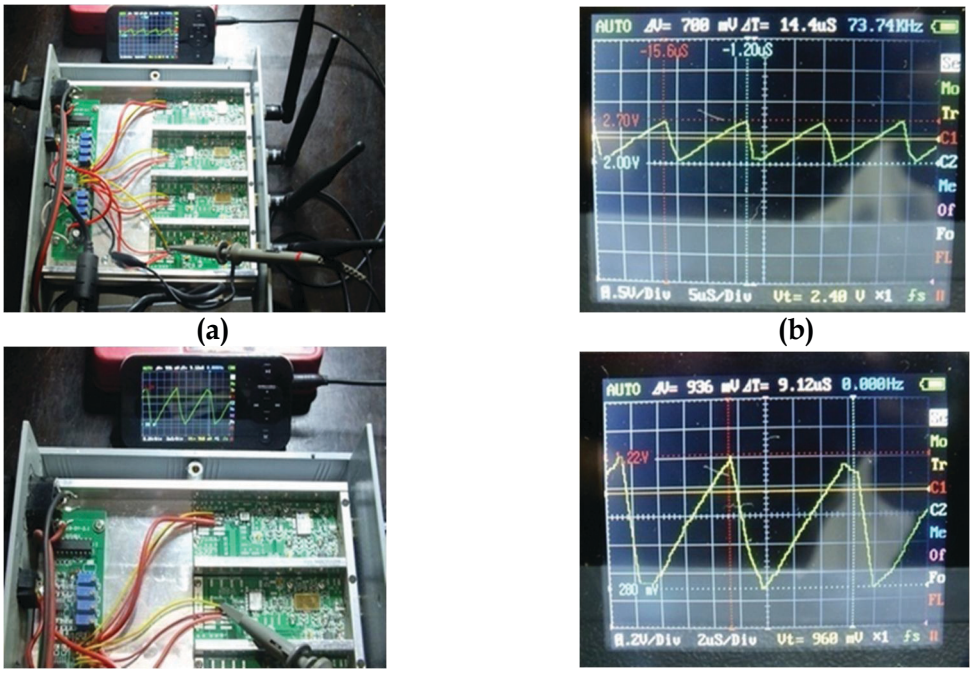
- Vmin = 2.00 V, producing F = 935 MHz
- Vmax = 2.70 V, producing F = 960 MHz and f = 73.74 KHz (disturbing the communication 73.74 thousand times per second)

For CDMA module, it is :

- Vmin = 0.28 V, producing F = 1900 MHz
- Vmax = 1.22 V, producing F = 1990 MHz and f = 109 KHz.

In the following picture can be seen the measurement results signal output module GSM and CDMA.

ISBN: 978-979-3220-41-3



(a) (b)

(c) (d)

Picture 4.2 Input Signal Measurement Module VCO + RF GSM Amplifier and Display measurement results.

Measurement of input signal in VCO module and RF amplifier for GSM network is done on RV9 and RV8 circuit to set Vmin and Vmax. RV8 and RV9 produce 935 and 960 MHz frequencies. There are also DCS1800 and 3G modules integrated into a module with GSM and CDMA.

Results of Jammer Range Testing

Based on the test results, it appears that GSM operators at a distance of 1 - 17 meters average jamming signal successfully with the category of no service (-), while the distance 18 - 19 meters emergency (x), and mobie can communicate (o) 20 - 21 meters. The following table below:

No	Provider / Distance (m)	Indosat (IM3)	Telkomsel (As)	XL	NTS Axis
1	1	-	-	-	-
2	2	-	-	-	-
3	3	-	-	-	-
4	4	-	-	-	-
5	5	-	-	-	-
6	6	-	-	-	-
7	7	-	-	-	-
8	8	-	-	-	-
9	9	-	-	-	-
10	10	-	-	-	-
11	11	-	-	-	-
12	12	-	-	-	-

ISBN: 978-979-3220-41-3

13	13	-	-	-	-
14	14	-	-	-	-
15	15	-	-	-	-
16	16	-	-	-	-
17	17	-	-	-	-
18	18	x	x	x	x
19	19	x	x	x	x
20	20	o	o	o	o
21	21	o	o	o	o

Table 4.1. Range of Jamming GSM signal using HP Mito 212

While CDMA operators which use Esia One Touch mobile there is no service (-) at a distance of 1 - 13 meters and there is service (o) at a distance of 14 - 21 meters. However, mobile ZTE C261 service is available at a distance of 1 - 21 meters. This is due to the lack of design tools, so the frequency of 1900 MHz communication is passed so that operators can communicate. The following table below:

No	Provider / Distance (m)	Smart ZTE C261	Flexi Esia
1	1	o	-
2	2	o	-
3	3	o	-
4	4	o	-
5	5	o	-
6	6	o	-
7	7	o	-
8	8	o	-
9	9	o	-
10	10	o	-
11	11	o	-
12	12	o	-
13	13	o	-
14	14	o	o
15	15	o	o
16	16	o	o
17	17	o	o
18	18	o	o
19	19	o	o
20	20	o	o
21	21	o	o

Table 4.2 Range of Jamming CDMA signal using Smart ZTE C261 and Flexi Esia Mobile Phone

5. Conclusion

Based on the design, testing, and analysis tools, it can be concluded that:

- Jamming tools that have been created can produce the same frequency with the existing frequency on Mobile Phone.

ISBN: 978-979-3220-41-3

- The greater the power be, the wider distance of the jamming radius covered will be
- Jamming tool that has been made able to jam GSM network in an area with a radius of 20 meters, CDMA flexi at a radius of 16 meters, and CDMA esia at a radius of 15 meters.

Suggestion

In the planning and manufacture that has been done it is suggested that in the next creation added the emitting power. It is intended that the range can be jammed further. It is also suggested that subsequent developments should pay attention to the selection of good antennas for the effectiveness of the jamming range.

Bibliography

Setiawan Denny, Direktorat Jenderal Sumber Daya dan Perangkat Pos dan Informatika, 2011.(Hal. 52-57).

Harianto, Subekti, "Rancang Bangun JammingGSM 900 dan 1800 Untuk Ruang Rapat", 2012. (Hal. 7, 11-15).

Ahmed Jisrawi, "GSM 900 Mobile Jammer", undergrad project, 2006 (Hal.11-15, 18-21).

Ahmed Sudqi Hussein Abdul-Rahman,Ahmad Nasr Raja Mohammad,"Dual Band Mobile Jammer for GSM 900 & GSM 1800",undergrad project, 2009 (Hal. 10-17).

http://digilib.ittelkom.ac.id retrivied on January 2014

http://123seminarsonly.com/Seminar-Reports/027/50135778-mobile-jammer.pdf retrivied on November 2013.

http://cobexonly.com/2008/05/frekuensi-cdma-800mhz-dan-1900mhz.html diakses retrivied on November 2013.

www.Mobile-online.com retrivied on November 2013.

http://www.electroschematics.com/1003/mobile-cell-phone-jammer/ retrivied on December 2013.

ISBN: 978-979-3220-41-3