ANTI-JAMMING TECHNOLOGY FOR MOBILE SIGNALS USING EMP JAMMER

Akash R Mannari
UG Scholar, Dept. of CSE, Rajarajeshwari College Of Engineering, Bengaluru, Karnataka, India
aakashmannari@gmail.com

ABSTRACT - _Networking‘ being an important aspect of every individual‘s daily life process. We being in the era of Wireless Sensor Networks, the security will be considered as the major susceptible to numerous types of attacks. These attacks come under the category – Denial Of Service attack (DOS attack). Jamming is one such attack which is categorized under DOS attack. This processes at the physical layer, preventing the legitimate nodes which are performing its function i.e. producing signals, decreasing its network performance. Hence, Anti-Jamming techniques have become essential for ensuring proper delivery of measured event (network signal). Nowadays the wireless networks are being more affordable; the Anti-Jammer can be built to disrupt the operation of the Electromagnetic Pulse jammer (EMP Jammer -DOS attack).Resilience to electromagnetic jamming, EMP jammer, and their function are considered to be the difficult problem. It is often very hard to distinguish between the network breakdown and its challenge to conceal the activity pattern.
Basically in wirelesses networking system, needs are functioned to take common sleep duration to extend their battery life, resulting in well-organized patterns created by communication process. The patterns can be in predicted intervals which are jammed by EMP jammers. Hence, in this paper, an instrument is being introduced, named as _Anti-Jammer‘. For the sensor networks (EMP jammers) this mechanism is time-synchronized and modified in such a way that with higher frequencies the patterns get detached resulting in proper working of the jammed device. Through analysis, simulation and experimentation this paper demonstrates that the Anti-Jammer device‘s efficiency of any EMP jammer which has the lowest censorship-to-link utilization ratio.

Keywords- Anti-Jammer, EMP Jammer, Wireless networking, DOS attack, ARM7, RTC

I. INTRODUCTION

Communication jamming devices were initially developed and used for military purposes. Mobile phones‘ nowadays being a most necessary gadget for an every individual uses it everywhere. In some of the organizations like Indian Space Research Organization (ISRO), Nuclear Power Plant the usage of mobile phones is prohibited; hence to obsolete these they use ―EMP JAMMERS‖, which is basically the electronic countermeasure device (EMC device) [1].

The technology used for cell phone jamming is very simple. The jamming device transmits an RF signal in the frequency range reserved for cell phones that interfere with the cell phone signal, which results in a "no network available" in your mobile display screen. The entire mobile phones network within that radius of the jammer is silenced. Using this technology any of the major organization can be signal-hacked (Gadgets using any kind of Radio wave signal can be hacked) very easily leading to a major chaos. Therefore, in this paper, the Antidote for the EMP JAMMER is being explained. This device jams the jammer and breaks down it. This method is called as ―ANTI-JAMMER‖. Mentioning that cell phone jammers are illegal devices in most countries, this report is solely done for educational purposes.

II. RELATED WORKS

A. Mobile Phone Jammer

A mobile phone- network jammer is basically an instrument used to prevent cellular phones from receiving signals from base stations. When we use that, the jammer meritoriously incapacitates cellular phones. These devices can be used realistically in any location, but are found predominantly in places where a phone call would be particularly disruptive because of various reasons. As with another radio jamming, cell phone jammers block cell phone use by sending out radio waves along with the similar range of frequencies that a normal phone use. This causes adequacy interference with the communication between the mobile networks and towers to render the phones inoperable. On most retail phones, the network would simply emerge out of range. Most of the mobile phones utilize various other bands to transmit and obtain communications from a tower (called frequency division duplexing, FDD). Jammers can strive by either obstreperous phone to tower frequencies or tower to phone frequencies. Smaller handheld models block all bands from 800 MHz to 1900 MHz within a 30-foot to 40-foot range (9-10 meters). Small devices tend to use the former method while superior, more extravagant models may interfere directly with the tower [2] [3].

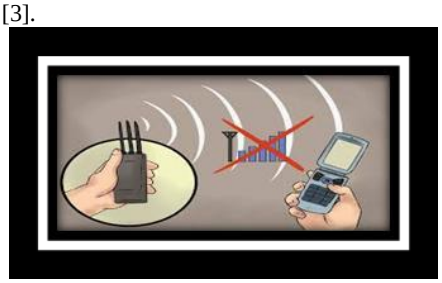

Figure1. Basic principle of Mobile jammer

The ambit of cell phone jammers can range from a dozen feet for mini models and micro models to kilometers for more extravagant models. The actual range of the jammer hinge on its power and the local surroundings, which may include any obstetrical that block the jamming signal. Less energy is required to disrupt signal from tower to a mobile phone than the signal from the mobile phone to the base station because the base station is located at larger distances from the jammer than the mobile phone and that is why the signal from the tower is not as strong. Earlier the EMP jammers were inadequate to working on mobiles phones which used only analog or any other older digital mobile phone standards. Newer models such as the double and triple band jammers can block all widely used systems (CDMA- Code Division Multiple Access, GSM- The Global System for Mobile Communication.) and are even very effective against newer phones which hop to different frequencies. [4][7].

Counter- Anti jammer encounters the jammed signal and breakdown the jammer circuit. The frequency will range more than 1800MHz resulting in breakage of the ionizer circuit used in the jammer, resulting in the normal functioning of the mobile networks.

1) Anti-Jamming Techniques:

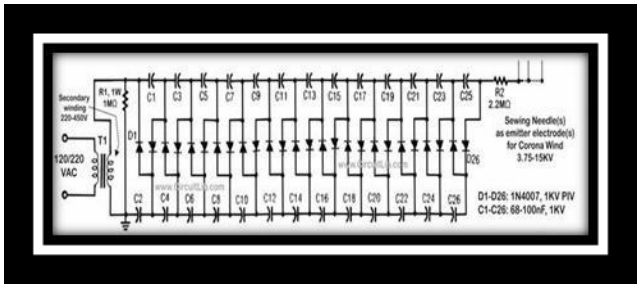

Figure2. Basic Circuit Diagram of an EMP JAMMER

When an anti-jammer is built the frequency generated will be extremely high, resulting in a breakdown of series connections of the capacitors. When the process of charging and discharging gets damaged the circuit of ―EMP JAMMER‖ breaks down and hence acquires the original state and the mobile regains its original signals. There are several ways to counter jamming an RF device.

	UPLINK (Handset Transmit)	**DOWNLINK** (Handset Receive)
GSM 900	890-915 MHz	935-960 MHz
DCS 1800	1710-1785 MHz	1805-1880 MHz

The three most common techniques can be categorized as follows:

Table I: Operating frequency bands

Anti-Spoofing:
Basically in this kind of jamming, the EMP Jammer forces the mobile to switch off automatically by itself. This type is very difficult to be implemented since the EMP Jamming device first detects any mobile phone network in that specific surrounding area, then the device sends the signal to disable the mobile phone. Some of the types of similar technique can perceive if a nearby mobile phone is there and sends a message to tell the user to switch the phone to the silent mode. Through this, any person can control your mobile from anywhere.

Counter- Firstly the mobile gets switched off and then gets switched on again (for which the reason is unknown to the user too), by the time gadget gets restarted the operator will get the access to the users mobile. The Anti-spoofing process takes quite a time to target the mobile and process the anti-jamming technology with it.

Shielding attacks:
This is known as ―TEMPEST‖ or ―Electromagnetic Field shielding (EMF shielding)‖. This kind of attacks requires a closed circumference in a Faraday range so that any electronic signal generating device inside this range will not be able to transmit or receive RF signal from the outer surrounding of that range.
Counter- In this process, the EMF shielding will be eliminated through the device. Hence, the gadget gets recovered.

Denial of service:
This technique is referred to DOS. In this technique, the device transmits a noise signal at the similar operating frequency of the mobile phone network in order to drop off the signal-to-noise ratio (SNR) of the mobile within its minimal value. This method of EMP Jamming technique is soft head one since the device is always switched on [5]. This device is of this type; Mobile jammer circuit includes IF section, RF section, Antenna, and Power supply. GSM, used in digital cellular and PCS-based systems, operates at the 900-MHz and 1800-MHz bands in Asia. Jammers can broadcast on any frequency and are effective against Aviation Mission Planning System (AMPS), CDMA, Time Division Multiple Access (TDMA), GSM, Personal Communication Services (PCS), DCS systems [6][8].

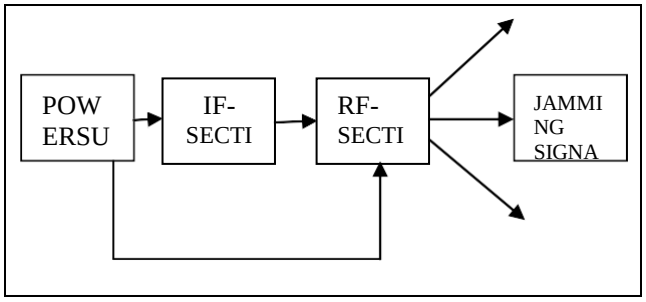

Figure3. Block diagram of JAMMER device

In our 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. So, our frequency design will be as follows:
GSM 900 ---- 960-1000 MHZ
GSM 1800--- 1885-1960 MHZ

B. ARM 7(LPC2148)
The ARM7TDMI-S is a general purpose 32-bit microprocessor, which offers high performance and very low power consumption. The ARM architecture is based on Reduced Instruction Set Computer (RISC) principles, and the instruction set and related decode mechanism are much simpler than those of microprogrammed Complex Instruction Set Computers. This simplicity results in a high instruction throughput and impressive real-time interrupt response from a small and cost-effective processor core. Pipeline techniques are employed so that all parts of the processing and memory systems can operate continuously. Typically, while one instruction is being executed, its successor is being decoded, and a third instruction is being
fetched from memory. The ARM7TDMI-S processor also employs a unique architectural strategy known as THUMB, which makes it ideally suited to high-volume applications with memory restrictions, or applications where code density is an issue. The key idea behind THUMB is that of a super-reduced instruction set. Essentially the ARM7TDMI-S processor has two instruction sets:
• The standard 32-bit ARM instruction set.
• A 16-bit THUMB instruction set.
The THUMB set‘s 16-bit instruction length allows it to approach twice the density of standard ARM code while retaining most of the ARM‘s performance advantage over a traditional 16-bit processor using 16-bit registers. This is possible because THUMB code operates on the same 32-bit register set as ARM code. THUMB code is able to provide up to 65% of the code size of an ARM, and 160% of the performance of an equivalent ARM processor connected to a 16-bit memory system.

C. REAL TIME CLOCK (RTC)

The real time clock (RTC) 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 an hour, minute, and second in addition to the date/calendar components of a 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.

D. Keypad

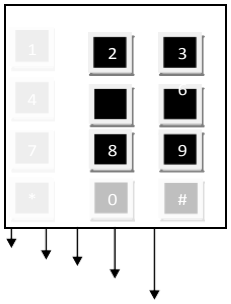

Figure4. 4x3 keypad structure

A basic 12 button keypad for user input. The buttons are set up in a matrix format. This allows a microcontroller to scan the 7 output pins to see which of the 12 buttons is being pressed. The jammer ON time and OFF time will be given with the help of keypad.

III. Result Analysis

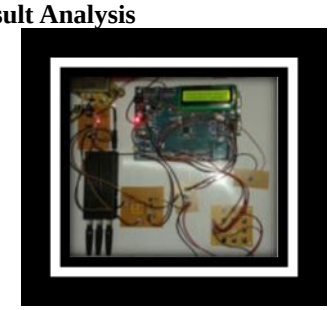

Figure5. Hardware design of the system

Figure6. Deactivation of mobile jammer and Activation of Anti-Jammer

Fig5 shows the hardware design of the mobile jammer with pre-scheduled time duration. It includes the Jammer, Anti-Jammer, ARM 7, keypad and relay. When the time schedule arrives in RTC the jammer will be activated with the help of relay and disrupt the communication system. This will be shown in fig6.

IV. CONCLUSION

This paper is successfully completed using Mobile jammer, Anti-Jammer, and ARM7. By this system, we can deactivate all the jammed signals at any location. This device can be applied in many places like;

- If the military Database is Jammed.
- In the War field, if the Radio signals are Jammed.
- In any of the organization where the signals might be jammed.

The design device works within the small range, with the proper installation and equipment; this can be transformed into a bigger device with a wider distance.

ACKNOWLEDGEMENT

The author gratefully acknowledges the support of management and Dr.Balakrishna R, Principal, RajaRajeshwari College of Engineering, Bengaluru, Dr.Usha Sakthivel, Professor, Head of Computer Science Department, RRCE, Bengaluru and my teachers and friends for their invaluable support and encouragement.

REFERENCES

[1] www.HowStuffWork.com

[2] En.wikipedia.org/wiki/Mobile_phone_jammer

[3] Multitopic conference2008.INMIC 2008.*IEEE* International

[4] "Zone of silence [cell phone jammer]," *Spectrum, IEEE, vol.42, no.5, 18*,May 2005

[5] Sami Azzam, Ahmad Hijazi, Ali Mahmoudy. ‖Smart Jammer for mobilephone systems‖

[6] Mobile & Personal Communications Committee of the Radio Advisory Board of Canada, –Use of jammer and disabler Devices for blocking PCS,Cellular & Related Services‖

[7]Ahmed Jisrawi, "GSM 900 Mobile Jammer", undergrad project, JUST,2006.

[8]John Scourias Overview of the global system for Mobile communications,http://ccnga.uwaterloo.ca/~jscouria/GSM/gsmreport.html#1

[9] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci, (2002) "A survey on sensor networks", IEEE Communication. Mag., pp. 102-114.

[10]Cagalj M; Capkun S; Hubaux J.P; (2007) "Wormhole-Base Antijamming Techniques in Sensor Networks," Mobile Computing, IEEE Transactions on, vol.6, no.1, pp.100-114.

[11] P.Naresh, P. Raveendra Babu, K.Satyaswathi; Dept of ECE, CMR College of Engineering&Technology Hyderabad, AP-India. –International Journal of Science, Engineering and Technology Research (IJSETR)‖ Mobile Phone Signal Jammer for GSM, CDMA with Pre-scheduled Time Duration using ARM7.