ISSN (Online) 2456 -1304

International Journal of Science, Engineering and Management (IJSEM)
Vol 2, Issue 12, December 2017

Implementation of Sniffers to Detect the Lost Mobiles

[1] P. Freny Hail Roy, [2] J. Antony Immaculate, [3] M. Lourdu Macrina
[1] III B.Sc, [2][3] II B.Sc.
[1][2][3] Dept of Computer Science, Holy Cross Home Science College, Tuticorin

Abstract:-- **The sniffer is a small base station. Transceiver section is seen in the sniffer. The frequency of the current cell and the frequency of the sniffer is different in which the operation of detection is being carried out. Some of the main important things are the frequency that has to be generated by the transceiver section is around 900MHz range which is a VHF range and it is necessarily to design the oscillator circuit for that frequency range. While designing the circuit of 900MHz frequency, it is important to provide cooling to the circuit. In the design of the sniffer, proper design of base station is important. Low power transmitter is seen in mobile phones and base station.. This implementation helps in the process of reducing the interference of the device and with the devices that are in the other cells.**

1. INTRODUCTION

Each and every day thousands of mobiles get misplaced or lost, though effective way for the blocking of the lost mobile to prevent unauthorized person from making and receiving the calls has been done by the manufacturers of the mobile with the help of International Mobile Equipment Identifier (IMEI) has been done but however there has been no development or very little progress for the detection of the misplaced mobile phone. For the detection of lost mobile SNIFFER plays a vital role .The sniffer device has to be designed precisely and size should be reduced for easy mobility for the purpose of detection.

What is Sniffer

The device can be called as a mobile Base station that includes Sniffer Base station, unidirectional antenna, tracking software. The sniffer is a small base station that includes transceiver section. It should operate at a frequency which is much different from the frequency of the current cell in which the operation of detection is being carried out. The directional antenna is an important device that is to be designed and used as it plays a major role. There are certain boundary conditions that have to be qualified for the identification of lost mobile like the power of the mobile should be good enough, the mobile phone should not be in the shadow region but however this method using modern technologies and devices. Our paper seems to be a bit costlier for initial setup but the cost is gradually reduced when effectively and efficiently utilized for the purpose of detection.

About IMEI

The GSM Mou's IMEI (International Mobile Equipment Identity) numbering system is a 15 digit unique code that is used to identify the GSM/DCS/PCS phone. When a phone is switched on, this unique IMEI number is transmitted and checked against a data base of black listed or grey listed phones in the network's EIR (Equipment ID Register). This EIR determines whether the phone can log on to the network to make and receive calls. To know the IMEI number the *#06# has to be pressed, the number will be displayed in the LCD screen it is unique to a mobile phone. If the EIR and IMEI number match, the networks can do a number of things.

Grey Listing and Black Listing:

1. Grey listing will allow the phone to be used, but it can be tracked to see who has it (via the SIM information).
2. Black listing the phone from being used on any network where there is an EIR match.

Designing of Sniffer

As stated this proposal is about the detection of lost mobile phone and for this purpose we are designing a new device called the Sniffer. The sniffer device has to be designed precisely and size should be reduced for easy mobility for the purpose of detection. The device can be called as a mobile base station that includes the following important components.

- Sniffer base station
- Design of unidirectional antenna
- Software for the tracking sniffer

ISSN (Online) 2456 -1304

International Journal of Science, Engineering and Management (IJSEM)
Vol 2, Issue 12, December 2017

Sniffer Base Station:

The sniffer is a small base station, it includes transceiver section. It should operate at a frequency that is much different from the frequency of the current cell in which the operation of detection is being carried out. Some of the main important things are the frequency that has to be generated by the transceiver section is around 900MHzrange which is a VHF range and it is necessarily to design the oscillator circuit for that frequency range .Another important is the cooling that has to be provided to the circuit while designing the circuit that is to be operated at 900MHz range of frequency. Hence proper design of base station is an important thing in the design of the sniffer. Mobile phones as well as the base station has low power transmitter is also transmitting at low power. The transmitter of the sniffer has to be a low power transmitter. This helps in the process of reducing the interference of the device with the devices that are in the other cells.

Design of unidirectional antenna:

Though the transceiver in a sniffer plays an important role in the detection of the mobile phone but however it is the directional antenna that has a major role in the design of the transmitter. The directional antenna acts as the eyes for the sniffer for the purpose of the detecting the lost mobile phones. Hence the proper design of the directional antenna is required. Antenna is a device which works at specified frequencies range for transmitting or receiving the data signal. In general, antennas transmit power depending on lobe pattern which varies from one antenna to the other. The lobe pattern is a two dimensional diagrams that is used to show radiation pattern. Radiation pattern of directional antenna.

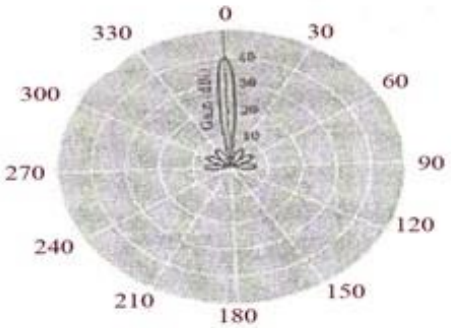


Fig Unidirection Antenna Radiation Pattern

In addition to this it is necessary that the transmitter should be a low power transmitter. The Gain and directivity are intimately related in antennas. The directivity of an antenna is a statement of how the RF energy is focused in one or two directions. Because the amount of RF energy remains the same, but is distributed over less area, the apparent signal strength is higher. This apparent increase in signal strength is the antenna gain. The gain is measured in decibels over either a dipole (dBd) or a theoretical construct called an Isotropic radiator (dBi).The isotropic radiator is a spherical signal source that radiates equally well in all directions. One way to view the Omni directional pattern is that it is a slice taken horizontally through the three dimensional sphere. The graphical representation of Radiation pattern of the unidirectional antenna is shown in figure. The spherical co-ordination system has three main components for the pattern representation and they are (R, _ , _) .The shape of the radiation system is independent of R, as long R is chosen to be sufficiently large and much greater than the wavelength as the largest dimension of the antenna. The magnitude of the field strength in any direction varies inversely with R. A complete radiation pattern requires the three dimensional representation. The other factors that are to be taken into account during the development of the antenna for the sniffer should be the gain and the directivity. As these features have a greater effect while designing the antenna. The gain of the antenna is defined as the ability of the antenna to radiate the power in a particular direction. The power radiated per unit area in any direction is given by the Pointing vector and is equivalent to E2/_2 W/m2 Total of the power that is being radiated by the antenna is given as W=_dThe average power that gets radiated is given as _(avg)=W/4_ (watts per Ste radian) The Directivity of the antenna is the direction in which there is maximum gain for the radiation that is being radiated, the gain of the antenna is given as a function of the angles. The directivity value is constant for a particular direction. In addition to the directivity and the gain of the antenna the other important thing that has to be taken into account is the power that is being radiated by the antenna. The total power is given as W and is the summation of the radiated power and the ohmic loss of the antenna. Here the Wl represents the ohmic losses of the antenna Wt=Wr+Wl The power gain of the antenna is given as gp=4__/wt The ratio of power to the directivity is referred as a measure of efficiency of the antenna gp/gd = Wr/(Wr+Wl) The power radiated by the antenna should be properly designed as this

ISSN (Online) 2456 -1304

International Journal of Science, Engineering and Management (IJSEM)
Vol 2, Issue 12, December 2017

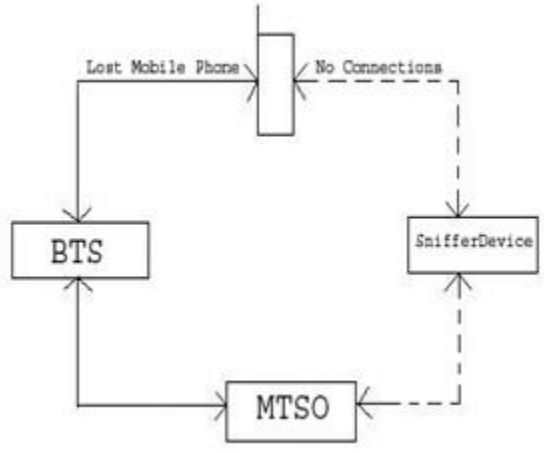
causes more penetration of the electromagnetic radiation and thus it might have some effect in the near by cells. The effective area of the antenna is another important factor that is mainly required in the receiving antenna and it may be referred as the effective aperture or capture area and is related to the directive gain of the antenna through the relation A=gd_2/4 Since the sniffer device that is constructed is a device that has both the transmitting and the receiving antenna. Effective gain has to be taken into account and this shows the ability of the antenna to capture the signal that the lost mobile is transmitting.

Software for Tracking:

The software part plays a major role in the tracking of the lost mobile phone It is the base for the antenna to track the lost mobile the main feature of this software is that it helps in the process of creation of the data base and this is mainly done using a Random Access Memory. The mobile phone that is lost has certain IMEI number that is embedded in the chip. This RAM of the sniffer device stores the IMEI number of the lost mobile phone. Thus this acts as a Data base or the directory of the lost mobile phone number/The software that is to be designed in such a way that the software has the in put as the IMEI number of the lost mobile phone from the RAM and this ID done u sing the SQL query that fetches the IMEI number. After getting the input of the lost mobile phones IMEI number it checks the comport for getting the information whether it obtains any signaling information from the lost device that might respond to the signal sent by the sniffer The programming is done with C or Java. However the C is most preferred as it is easily embedded with the chips. With V B the front end is designed. The oracle SQL is the back end as it helps in retrieving the input data from the RAM using the query. But however the sample program that we have designed does not use the oracle it takes the input directly from the keyboard and this is an example and a dummy program that has been created that helps in the understanding of how the device would work.

Working of Sniffer Device:

The sniffer is basically a transceiver that works in the frequency which is in the special unused range that is operated by the service provided or it can designed to operate at a frequency that is of much different frequency than the one that is being used by the nearby cells as there may be possibility of interference by the device with the devices in the nearby cells. The working for the device is as follows. The normal operation of the mobile with the base station and there is a BTS that acts as a middle man in the process of communication between the mobile and the MTSO which is popularly known as MSC or Mobile Switching Centre .There is always a two way communication between devices and before the establishment of the communication the authentication of the SIM card that has the IMSI or the International Mobile Subscriber Identifier .This IMSI number helps in the authorization of the user. The second authentication is the authentication of the handset, which is done in EIR or the Equipment Identifier Register. This register is located at the MSC and it contains the IMEI number of the lost handset and if the signal is obtained from the normal one then the two way communication is established. The IMEI of the lost mobile phone number once has been reported to the service provider, who keeps in track of the record of lost mobile phones. The MTSO or the MSC which keeps in track of all the mobile phones with IMEI number and the IMSI number has the information of the lost mobile phones location which means the location of the cell where the lost device is because of the two way communication with the device the BTS of the lost device is known to MSC. From this information regarding the cell in which the device is located the sniffer device is introduced.



The initial connection between the cellular network and lost mobile phone The next figure or the fig 2 shows the sniffer that gets into work for the purpose of detection of the lost device. After the information regarding the IMEI number of the lost device is provided by the MTSO or MSC .This is then fed into the sniffers main memory the sniffer's located in particular cell gets into action of detecting the lost device.

ISSN (Online) 2456 -1304

International Journal of Science, Engineering and Management (IJSEM)
Vol 2, Issue 12, December 2017

The sniffer uses a frequency that is different from the one that is being used by the base station and the located nearby cells .The base station disconnects the connection with the lost mobile phone, as there is a request regarding this action from the EIR part of the MSC. This causes the lost device to search the BTS to get locked with since each base station does not have authorization capability the lost devices end appropriate connection request signal. Now when the sniffer device is being deployed and this device has in built authorization capability the lost device finds the sniffer to get itself locked to the frequency of the sniffer .While the connection between the sniffer and the mobile phone is established; the IMEI of the lost mobile is validated with the stored IMEI and after successful authorization the communication between the sniffer and the lost device is established. If the other devices in the same try to communicate with the sniffer the access is denied and this is done at the validation done based on the IME. Once the communication starts it is mainly with the antenna and the signal strength of the lost device the location can be tracked. However the process to searching can also be aided with the GPS system for more accurate and fast detection The main requirement is that the sniffer is operated in a frequency that is different from the frequency adopted by the cell and nearby ones. Hence the interference from the nearby cell can be avoided. The directional antenna is used in finding the location of the mobile phone.

Advantages:

- Find lost mobile phones effectively
- Easy to design
- It uses frequency to find lost mobiles

Disadvantages:

- It includes cost
- No prevention from police force
- Sometimes a dangerous job

Limitations:

- Power of mobile should be good enough
- Mobile should not been in shadow region

Potential Drawback:

Due to complexity and cost issues involved in this process, such a device may prove beneficial when used for lost detection. The concept for sniffers for detecting lost mobiles paves a way to recovery for lost mobiles. So once the pricing and complexity of implementation can be brought down to reasonable levels, no one can except to see of practical implementation over next few years.

CONCLUSION:

Since the boom of the mobile phone for the purpose of the communication there has been a large no. of complaints regarding the mobile phone that is being lost and there has been no effective method developed for detecting the lost device. The given paper dealt about the idea of development "Sniffer for the detection of lost Mobile phones" paves a way by means of which the lost mobile phones can be recovered. But the process of detection is yet to be developed through the software and demo has been developed and is with the authors. The demo has been written in VB that gives the over view of how the lost mobile is being detected and the software has been written in C. The SQL has to be used for the purpose of querying and the internal architecture is of lesser complexity compared to the base station as this mainly involves the control signal and there is no need for the voice process. The design involved the following: Design of the sniffer base station design of unidirectional l antenna, development of software for tracking. Though this method appears to be a little bit complex involving the design of the sniffer but however for large scale detection the overall effective cost of the design and the detection scales down. There are certain boundary conditions or criteria that have to be qualified for the identification of the lost mobile like the power of the mobile should be good enough, the mobile phone should not be in the shadow region etc., but however this method can be improved by using modern technologies and devices