International Journal of Advanced Technology & Engineering Research (IJATER)
www.ijater.com

SNIFFER TECHNOLOGY FOR DETECTING LOST MOBILE

N. Rohit[1], L. Prudhvi[2]
[1]N. Rohit & Shruti Bhargava Choubey
SREENIDHI INSTITUTE OF SCIENCE AND
TECHNOLOGY, YAMANAMPET, GHATKESAR, HYDERABAD
[2]L. Prudhvi & SREENIDHI INSTITUTE OF SCIENCE AND
TECHNOLOGY, YAMANAMPET, GHATKESAR, HYDERABAD
[1]rohitnukala1@gmail.com
[2]lagishettyprudhvi30@gmail.com

***Abstract*— SNIFFER is One of the most interesting things about cell phone is that it is really a radio an extremely sophisticated radio, which uses some band of frequency that has the basic working similar to the ordinary cordless phone. The mobile cellular communication has been appreciated since its birth in the early 70's and the advancement in the field of VLSI has helped in designing less power, smaller size but efficient transceiver for the purpose of communication. In this paper we discuss the problem and the probable solution that could be done. The IMEI number is a unique number that is embedded in the mobile phone the main purpose of which is the blocking of calls that is made by unauthorized person once the mobile is reported as stolen but here we use it effectively for the purpose of detection.some of the impartent things are frequency that has to be generated by the transceiver section.the transmitter of the sniffer has to be a low power transmitter.this help in process of reducing the interference of the device with the device that are in the other cell.**

***Keywords*— sniffer, IMEI, base station, high gain unidirectional antenna, MTSO (mobile telephone switching office).**

I. INTRODUCTION

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. For example grey list or black list a phone

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.
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 dirrecton.

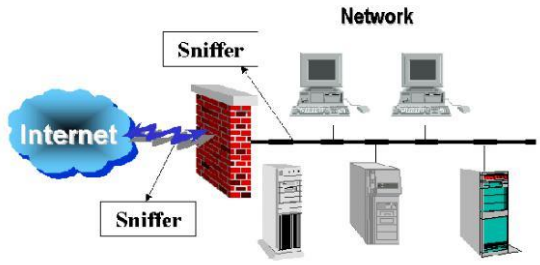

Fig 1.1 sniffer network

II. LITERATURE SURVEY

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. Software for the tracking, 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.

Fig 2.1 Sniffer box

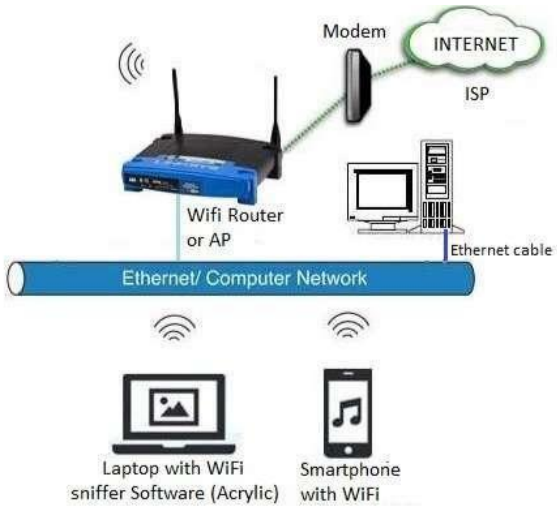

Fig 2.2 Ethernet computer network

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 is shown in fig. 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 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.

III. EXISTING METHODOLOGY

On wired shared medias networks such as Ethernet, token rings, and FDDI networks, depending on their network structure it may be possible to capture all traffic on the network from a single machine on the network. On modern networks, traffic can be captured using a network switch with a so-called *monitoring port* that mirrors all packets that pass through designated ports of the switch. A network tap is an even more reliable solution than to use a monitoring port, since taps are less likely to drop packets during high traffic load. On wireless LANs, traffic can be captured on one channel at a time, or by using multiple adapters, on several channels simultaneously. On wired broadcast and wireless LANs, to capture unicast traffic between other machines, the network adapter capturing the traffic must be in promiscuous mode. On wireless LANs, even if the adapter is in promiscuous mode, packets not for the service set the adapter is configured for are usually ignored.

When traffic is captured, either the entire contents of packets are recorded, or just the headers are recorded. Recording just headers reduces storage requirements, and avoids some legal issues, yet often provides sufficient information to diagnose problems. Captured information is decoded from raw digital form into a human-readable format that lets users easily review exchanged information. Protocol analyzers vary in their abilities to display and analyze data.Some protocol analyzers can also generate traffic and thus act as the reference device. These can act as protocol testers. Such testers generate protocol-correct traffic for functional testing, and may also have the ability to deliberately introduce errors to test the DUT's ability to handle.

Protocol analyzers can also be hardware-based, either in probe format or, as is increasingly common, combined with a disk array. These devices record packets (or a slice of the packet) to a disk array. This allows historical forensic analysis of packets without users having to recreate any fault 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 signalling 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.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.

IV. PROPOSED METHODOLOGY

Here the signal strength of the received signal is obtain antenna pattern is plotted once the signal of the mobile is obtained. The no. of antenna pattern for different position of same mobile phone is used to find the exact location. But however in this method the directional antenna used much be of a very small beam width this helps in more accurate process of detectionThe 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 fig 2 &3shows the working of the sniffer ;as given in the fig2 it gives 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 theestablishment 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 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. 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.

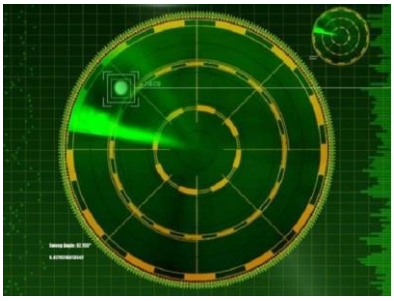

Fig 4.1 working scheme

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 IMEI. 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 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. 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 phone.

Fig 4.2 connection diagram

Smart antenna patterns are controlled via algorithms based upon certain criteria. These criteria could be maximizing the signal-to-interference ratio (SIR), minimizing the variance, minimizing the mean-square error (MSE), steering toward a signal of interest, nulling the interfering signals, or tracking a moving emitter to name a few. The implementation of these algorithms can be performed electronically through analog devices but it is generally more easily performed using digital signal processing. This requires that the array outputs be digitized through the use of an A/D converter. This digitization can be performed at either IF or baseband frequencies. Since an antenna pat-tern (or beam) is formed by digital signal processing, this process is often referred to as digital beam-forming.

V. COMPARISON OF PROPOSED METHODOLOGY WITH EXISTING METHODOLOGY

Each and every technology has its own merits and demerits, at times the merits overcome the demerits and at other it is vice versa. Though the sniffer device for the mobile phones has it's own merits in terms for the of using the IMEI number for the detection of lost mobile, the frequency that it uses is high frequency in the range of 850-950 MHZ where there is a slight effect of the reflection of the signal from the ground, but however the effect is less pronounced and the other demerit here is that even though the directivity of the antenna is less the distance of the propagation should be restricted and the device is handheld and automated one. But however this new

technique that provides a light for the detection of the lost mobile phones.

Because network sniffers are able to monitor all traffic passing through a connection, they are very useful for monitoring and analysis of a specific network. Networks are becoming more and more complicated as they expand, and it's a very time consuming and tiresome task to pin point a problem. New technology for network sniffers now allows network administrators to capture, decode, and analyze packets in real time. With this technology, a system captures packets off the network, decodes them into human-readable format, runs the packet through an expert system for analysis, and finally displays the information to the administrator. Today a network administrator might be alerted to a network issue before users experience any significant problems. In Ether Peek NX, for example, packets can be grouped together by source address, destination address, port, conversation, and protocol tokens. With this feature, analyzing specific network communications no longer requires poring over logs and having hard time searching in a log file, but is as easy as a click of the mouse.

VI. CONCLUSIONS AND FUTURE DIRECTIONS

This paper gives the brief idea aboutSniffer technology is very useful in case of the mobile stealing. This technology works on the frequency that is usually used for military purposes. The technology contains its tracking softwares that make it very popular among theft detecting techniques. The design involved the following steps: · Design of a sniffer base station. · Design of unidirectional antenna. · Development of software for tracking a lost mobile phone. The idea of development "Sniffer for the detection of lost Mobile phones" paves away by means of which the lost mobile phones can be recovered. Let all of us hope for the advancement of the technology in this domain which will be very helpful for each and every persons who are lost mobiles. Though this method appears little bit complex involving the design of the sniffer but however the large-scale detection the overall effective cost of the design and detection scales down. Though there are certain boundary conditions or criteria 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 etc., but however this method can be improved by using modern technologies and devices.

REFERENCES

[1] Network Sniffers, Alan Joch, 2001(Intro&Use.doc).
[2] Schiller, "Mobile Communication", Pearson Education 1 Edition, 7th reprint -2003. •
[3] S. Satya Sri Ambica, P. Padma Priya, Dr.N.Srinivasu, "Sniffer Technology to Detect Lost Mobile ", International Journal of Engineering Trends & Technology, volume 4,issue4 –April 2013.
[4] uthiyavan,U., "EnhancingUser Privacy-Location Based Search Using MEMD" , IEEE International Conference onPortable Information Devices 2007, May 2007, Pp-1-5.
[5] Ansari, S., Rajeev, S., &Chandrashekar, H. PacketSniffing(2002). A Brief Introduction. IEEE Potentials (Vol. 21, Issue 5,pp. 17-19).
[6] Asrodia, P. & Patel, H. (2012). Network Traffic Analysis UsingPacket Sniffer International Journal of Engineering Research andApplications (IJERA) ISSN: 2248-9622 www.ijera.com (Vol. 2,3, pp.854-856)