Sniffeer Technology for Mobiles

Poonam Singla

Abstract: The cell phone though the mobile communication system is proved to be an advantageous method of communication over wired communication, there is another problem that is the mobile phones get lost or get misplaced. The losses are increasing day by day and there has been very little effort that has been done to obtain the lost mobile phone. The main scope for this paper is "The proposal for the detection for the lost mobile phones." Every day over thousand of mobile phones get misplaced and lost, though an effective way for the blocking of the lost mobile to prevent unwanted user has been done by the manufacturers of the mobile by usage of International Mobile Equipment Identifier (IMEI) has been done but however there has been no development or very little progress in this area to find the misplaced mobile phones.

Keywords: International Mobile Equipment Identifier (IMEI), Detection

I. INTRODUCTION

Each and every day thousands of mobiles get misplaced or lost. To prevent unauthorized person from making and receiving the calls we use this technique. The effective way for the blocking of the lost mobile with the help of International Mobile Equipment Identifier (IMEI). The device can be called as a mobile Base station that includes Sniffer. The losses are increasing day by day there has been very little effort that has been done to obtain the lost mobile phone. My paper "Sniffer for Mobile Phones" proposes a path for solving this problem. The IMEI number embedded in the mobile phone that has been used for blocking calls it effectively utilized for the purpose of detection. The Sniffer is basically a transceiver that works in the different frequency that we are commonly used. The sniffer device has to be designed precisely and size should be reduced for easy mobility for the purpose of detection

II. LITERATURE REVIEW

Abdelallah and Elhad (2002) concluded that sniffer combines searching for machine in promiscuous mode and using honey pot to detect potential use of sniffed information. Hence, Sniffer Wall covers online detection as well as after the fact or *information replay* detection regardless of the platform. In addition, the detection based on MAC addressing makes it possible to detect any machine of the networkwhich is in promiscuous mode for all Windows platform (9x/ME, NT/2000) or on Linux platforms (kernel /2.0 to 2.4).

Remo and Ogun concluded that there are many available tools used to capture network traffic, but there are limitations in some of the tools. Some tools only capture network traffic without analysis, whilesome require large memory size for installation therefore the researcher has to use other tools for analysis to get the traffic features as required and also consider the memory size of the system in use. Our system captures network traffic and analyzes it and allows the user to take only the features he needs. Our system requires little memory size for installation and enables the user to store his/her selected features in a file for later use in his/her work. Consequently, this will reduce the memory that is used to store the data. Finally, P Sniffer contains additional Functionalities like 3D pie chart statistics and possible malicious IP address detection.

Patil at el. (2014) concluded that In this paper the android application for tracking the mobile phones is created and installed in a mobile phones system. This application basically works with the help of in built GPS in the mobile phones. When the unknown user tries to change the SIM card in that mobile phone, the current longitude and latitude information is sent as SMS to the specified phone number without the knowledge of user. Using the longitude and latitude values the exact location can be found using Google maps.

Lomet at el. (2001) gave their view that If you are currently a Sniffer customer or are considering solutions from Sniffer Technologies,you may not have been aware of the additional security features that can be used to compliment your security defenses. Furthermore, the ability to leverage existing technologies in new ways offers a powerful mans of enhancing network security performance without impacting budgets. Portable and Distributed from Network Associates can offer users more than just a means of maximizing network performance and uptime – they can help secure your network infrastructure before, during and after an attack. At Sniffer Technologies, we are proud to apply our network analysis expertise to provide customers with solutions to all of their network management and security needs.

Arvind and Negi (2012) concluded that with the help of Sniffer Program a programmer can listen computer conversation. It is the best method of detecting lost mobile. In general 42% of lost mobiles have no security in place to protect data • 20% of lost devices had access to work email • 20% contained sensitive personal information such as national insurance numbers, addresses and dates of birth • 35% had access to social networking accounts via apps or web browser. Period 2004-2011, by focusing on high-level attacks, such those to user applications. We group existing approaches aimed at protecting mobile devices against these classes of

attacks into different categories, based upon the detection principles, architectures, collected data and operating systems, especially focusing on IDS-based models and tools. With this categorization we aim to provide an easy and concise view of the underlying model adopted by each approach.

Shankar and Mahesh (2013) viewed that Distributed computing involving several computers in a network can be achieved using message passing or remote procedure calls (RPC). The recently developed mobile agent technology

Add a new dimension to distributed computing. Experts suggest that mobile agents will be used in many Internet applications in the years to come.However there still exist many technical hurdles that need to be tackled, the most important of them being security. Only when security issues are properly addressed, will the mobile agent Technology is widely accepted. However if intruder makes some changes in our mobile agent platform or mobile agent, then it may fail the whole process. So in future, some more security measures should be taken for the guaranteed security. Mobile agent selects any node randomly and investigates that node, if it finds excessive incoming traffic on the network interface card then report to network administrator. So the sniffer can be detected.

Gupta (2013) concluded that Capturing, or sniffing, network traffic is invaluable for network administrators troubleshooting network problems, security engineers investigating network security issues, developers debugging communication protocol implementations, or anyone trying to learn how their networks work. Because attackers use sniffers for network reconnaissance and to intercept transmitted credentials and data, learning about the capabilities and limitations of packet sniffers is an important facet of understanding the security risks.

Khan (2012) concluded that the network configuration is hidden form normal users. Network users do not have any information about nature of network. So, users of the network may invoke sniffer detection technique which is not effective in that environment. This sniffer detection technique provides wrong information to user which may be dangerous for him. Our proposed invocation module checks the nature of environment automatically and then invokes appropriate sniffer detection technique for that environment. If environment is broadcast then ARP cache poisoning detection technique is invoked. If environment is not broadcast then enhanced Switched network sniffer detection based on IP packet routing detection technique is invoked to detect a sniffer. Both detection techniques are effective to detect active as well as passive sniffer. With the help of this invocation module it is possible to detect passive as well as active sniffer hosts in both environments automatically. Currently, we are working on detection of an actives witch sniffer that does not response any type of ICMP echo request packet.

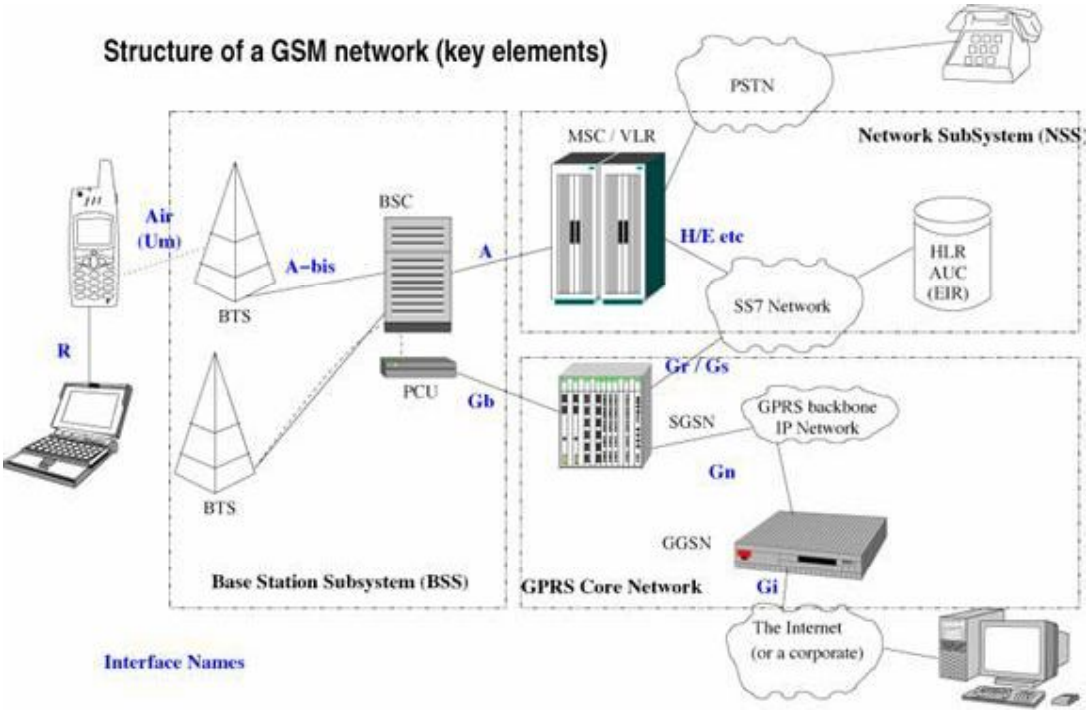
Kulshrestha and Dubey (2014) viewed that after studying various research papers, it is concluded that sniffing is a major attack on websites or in other words it is a major threat to browsing. Sniffing attack is very difficult to detect, but once this attack is detected then it can easily be quarantined. It is better to take precautions because it cannot be cured. Various research papers also describe about flash work in which MIME type file can be converted into HTML type. The filters are attached in the network so that it can filter the unauthorized access. Since the security measures are costly so it can't be possible for small scale organization. With the help of triggers it is easy to secure connection for complex authentication also. This prevents attacks like sniffing; shoulder surfing, overhearing, dumpster driving. Password shaving alpha-numeric characters are made to secure connection. Various algorithms are used to prevent sniffing. Browser content sniffing algorithms are also used to provide defence against content sniffing XSS. In nutshell, it is concluded that sniffing can be controlled by using different variety of filter for different sniffing attacks.

III. OBJECTIVE

My aim is to find the lost mobile using IMEI number of phones.

A Brief Introduction to GSM:

Global System for Mobile Communications (GSM) is the most popular mobile phone system in the world. The Cellular Operators Association of India (COAI) has released its GSM subscriber figures for the month of February 2013. As per the figures, the total number of GSM subscribers at the end of February 2013 stood at 655.59 million. It notes that the number of subscribers in this segment fell by 1.97 million in February 2013, thereby registering a drop of 0.30 percent from the previous month. The name GSM first comes from a group called Group Special Mobile (GSM), which was formed in 1982 by the European Conference of Post and Telecommunications Administrations (CEPT) to develop a pan-European cellular system that would replace the many existing incompatible cellular systems already in place in Europe. But when GSM service started in 1991, the abbreviation "GSM" was renamed to Global System for Mobile Communications from Group Special Mobile. The typical architecture of GSM network was shown in figure :



(Fig.1.The architecture of GSM)

The GSM network can be divided into three parts.
1. The Mobile Station carries the subscriber.
2. The Base Station Subsystem controls the radio link with the Mobile Station.
3.The Network Subsystem, the main part of which is the Mobile services Switching Centre, performs the switching of calls between the mobile and other fixed or mobile network users, as well as management of mobile services, such as authentication. Not shown is the Operations and Maintenance centre, which oversees the proper operation and setup of the network. The Mobile Station and the Base Station Subsystem communicate across the air interface or radio link. The Base Station Subsystem and the Network Subsystem are also called the fixed network.

a) Mobile Station:

The mobile station (MS) consists of mobile equipment and a Subscriber Identity Module (SIM) card. The most common mobile equipment is the mobile phone. By inserting the SIM card into a cellular phone, the user is able to receive calls at that phone, make calls from that phone, or receive other subscribed services. The mobile equipment uniquely identifies the International Mobile Equipment Identity (IMEI).

The SIM card stores the sensitive information such as the International Mobile Subscriber Identity (IMSI), Ki (a secret key for authentication), and other user information. All this information may be protected by personal identity number (PIN). The SIM card itself is a smart card and is in accordance with the smart card standard (ISO 7816-1, -2). The GSM 11.11 has the detailed specification about the SIM card.

b) Base Station Subsystem

The Base Station Subsystem consists of the Base Transceiver Station (BTS) and the Base Station Controller (BSC). The Base Transceiver Station houses the radio transceivers that define a cell and handles the Radio link protocols with the Mobile Station. In a large urban area, there will potentially be a large number of BTS deployed. The Base Station Controller manages the radio resources for one or more BTS. It handles Radio channel Setup, frequency hopping, and handovers. The BSC is the connection between the mobile and the Mobile service Switching Centre (MSC). The BSC also translates the 13 kbps voice channel used over the radio link to the standard 64 kbps channel used by the Public Switched Telephone Network or ISDN.

c) Network Subsystem:

The central component of the Network Subsystem is the Mobile services Switching Centre (MSC). It acts like a normal switching node of the PSTN or ISDN, and in addition provides all the functionality needed to handle a mobile subscriber, such as registration, authentication, location updating, handovers, and call routing to a roaming subscriber. These services are provided in conjunction with several functional entities, which together form the Network Subsystem. The MSC provides the connection to the public fixed network (PSTN or ISDN),

and signalling between functional entities uses the ITUT Signalling System Number 7 (SS7). The Home Location Register (HLR) and Visitor Location Register (VLR), together with the MSC, provide the Call routing and (possibly international) roaming capabilities of GSM. The HLR contains all the administrative information of each subscriber registered in the corresponding GSM network, along with the current location of the mobile. There is logically one HLR per GSM network, but it may be implemented as a distributed database. The Visitor Location Register contains selected administrative information from the HLR, necessary for call control and provision of the subscribed services, for each mobile currently located in the geographical area controlled by the VLR. Although each functional entity can be implemented as an independent unit, most manufacturers of switching equipment implement one VLR together with one MSC, so that the geographical area controlled by the MSC corresponds to that controlled by the VLR. The other two registers are used for authentication and security purposes. The Equipment Identity Register (EIR) is a database that contains a list of all valid mobile equipment on the network, where each mobile station is identified by its International Mobile Equipment Identity (IMEI). An IMEI is marked as invalid if it has been reported stolen or is not type approved. The Authentication Centre is a protected database that stores a copy of the secret key stored in each subscriber's SIM card, which is used for authentication and ciphering of the radio channel.

IV. CONCEPT OF CHANNEL IN MOBILE COMMUNICATION:

The channel in the mobile communication refers to the frequency that is being used for the purpose of communication. Generally there are two types of channel in mobile communication. One of the channels is the traffic channel (physical channel) and the control channel. The physical channel is used for transmission of the voice data and the signalling information. The physical channel carries different massages to be sent. These are called as the logical channel.

a) Broadcast Control Channel (BCCH):

The BCCH is transmitted by a Base Transceiver Station (BTS) to provide the signalling information required by the MS (Mobile Station) to access and identify the network. The BCCH will include information such as the LAC (Location Area Code). When the MS are switched on the MS searches for the BTS, it scans the entire channel. It scans the list of entire frequency that is allotted to the service provider .It finds a strongest carrier it checks if it is a control channel. It does so by searching a particular logical channel called as broadcast control channel (BCCH). The frequency carrying BCCH contains important information like LA identity, synchronization information and network identity. Without such information the MS cannot work in the network. The information is broadcast at regular interval leading to broadcast control channel (BCCH) When the MS finishes analyzing the information in BCCH; it then has the information to work with the network. However the MS roams to another cell, it must repeat the process of reading FCCH, BCCH in the new cell. If the mobile subscriber then wishes to make or receive a call, the common control channel (CCCH) must be used.

b) TRAFFIC CHANNEL (TCH):

Ones the call set up procedure has been done or completed on the control physical channel, the MS tunes to traffic physical channel. It uses the traffic channel (TCH).

There are two types of traffic channel (TCH):

- The full rate TCH: It transmits full rate speech (13 kbit/ sec). A full rate TCH occupies one physical channel.
- Half rate TCH: It transmits half rate speech (6.5 kbits/sec). Two half rate TCH can share one physical channel, thus doubling the capacity of the channel.

V. CONCEPT OF IMEI:

a)Mobile security with IMEI:

With mobile phones becoming the popular target of thieves, it becomes important for subscribers to get acquainted with some practical measures to keep their mobiles safe. One of the most important one happens to be the International Mobile Equipment Identity (IMEI). In case a mobile phone is stolen, all that a subscriber has to do is call the network service provider, explain about the theft and give the IMEI. The network will immediately deactivate the stolen phone's SIM card to prevent unauthorized calls being made. IMEI is a unique 15-digit code used to identify an individual GSM mobile telephone to a mobile network. It can be displayed on most phones by dialing ***#06#.** The code is also printed on the compliance plate under the battery. The number consists of four groups that look like this:

nnnnnn--nn-nnnnnn-n .

The first set of numbers is the Type Approval Code (TAC) which will give you mobile brand and model. Others are given by manufacturer (6 digits are serial number and 1 is check digit).The first two digits represent the country code. The rest make up the final assembly code. And the second group of numbers identifies the manufacturer. The third set is the serial number and the last single digit is an additional number (usually 0). IMEI numbers of cellular phones connected to a GSM network are stored in a database (EIR-Equipment Identity Register) containing all valid mobile phone equipment. Whenever a phone logs onto a particular network to

make or receive calls, its IMEI number is emitted and gets registered. In case of stolen phones, the service provider can pass on the information to the police. They will further trace the user through the SIM card. *"However, this technology is not available in Code Division Multiple Access (CDMA) mobiles"*.

b) WHAT IS AN IMEI NUMBER:

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 to a GSM/DCS/PCS network.

When a phone is switched on, this unique IMEI number is transmitted and checked against a database of blacklisted or greylisted phones in the network's EIR (Equipment ID Register). This EIR determines whether the phone can log onto the network to make and receive calls.

c)How to display a phone's IMEI number:

Type ***#06#** on the keypad. This code works on most phones.

d) What effect does a listing of an IEMI number with an EIR have?

If the EIR and IMEI numbers match, the networks can do a number of things. They can for example greylist or blacklist a phone: **Greylisting** will allow the phone to be used, but it can be tracked to see who has it (via the SIM info). **Blacklisting** bars the phone from being used on any network where there is an EIR match.

e) IEMI Example:

490154100837810

490154	Type Approval Code (TAC) The first two digits is the code for the country approval.

f) Final Assembly Code (FAC)

01,02	AEG
07 , 40	Motorola
10, 20	Nokia
30	Ericsson
40, 41, 44	Siemens
47	Option International
50	Bosch
51	Sony
51	Siemens
51	Ericsson
60	Alcatel
70	Sagem
75	Dancall
80	Philips
85	Panasonic

083781 - Phone Serial Number

0 - Additional Number

VI. BLACKLISTED OR BARRED HANDSETS

a) What is it all about???

A phone may be blacklisted (or barred) for many different reasons, but the most common reason is that it has been reported either lost or stolen! It is only the networks (Orange, T-Mobile, O2, Vodafone etc) that have the facility to blacklist a handset.

If you are unfortunate enough to either lose or even worse have your phone stolen you should report it to your service provider (your network) immediately Your service provider can then blacklist the handset so that it can no longer be used to make or receive any calls. The networks do this by adding your phones serial number onto a national blacklist database (Central Equipment Identity Register). Effectively the handset becomes absolutely useless and the thief is in possession of a pretty paperweight! :-))

b) So How Does Blacklisting Work?

Every mobile phone has a unique serial number. This serial number is called the IMEI number (International Mobile Equipment Identity). It can normally be found underneath the phones battery and it is 15 digits long.

Now each time you switch your phone on or attempt to make a call the network systems check the IMEI number of the handset you are using. At this point the IMEI number of your handset is cross-referenced with the Central Equipment Identity Register. If the IMEI number of your handset is on the CEIR then the network will either:

1) Refuse to send a signal to your phone (No signal strength at all)

2) OR WILL supply a signal but will not allow any outgoing or Incoming calls.

If your IMEI number is on the CEIR your handset is blacklisted and therefore useless. By spreading the word that "**stolen handsets will not work**" it is hoped that street crime can be reduced!

c) How to Check If Your Phone is blacklisted!!

Different networks blacklist handsets in different ways:

□□□□□□□□□□□□□□□□

If you place an active orange or O2 sim into a blacklisted handset your phone will not show any signal strength at all! If the handset is a Nokia then a "**SIM card registration failed**" message will also be displayed. If your handset is an Ericsson then an "**Invalid Mobile**" message will be displayed. For most other manufacturers the handset will simply show no signal!

Vodafone & T-Mobile

If you place an active Vodafone or T-Mobile sim into a blacklisted handset, the phone will appear to function perfectly UNTIL you try to make an outgoing call. When you try to call out from the handset you will hear a sequence of beeps and then the call will be dropped!!

d) Unlocking & blacklisting, is there any Connection?

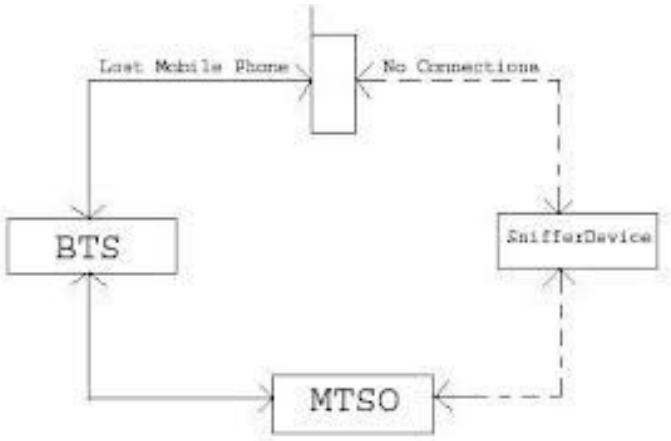
The answer is that there **used** to be a connection before O2 and Vodafone started blacklisting handsets! Orange and T-Mobile have been blacklisting handsets for a long time (It is only recently that O2 and Vodafone also started blacklisting handsets). NB Orange & T-Mobile always lock their handsets!(e.g. an Orange handset will only accept an Orange sim and will not accept an O2, Voda or T-Mobile sim)

So if you reported your Orange or T-Mobile handset missing to your network it became barred/blacklisted! BUT it was only barred on your home network. Therefore unlocking the barred handset would enable it to work on every network except the one it was originally locked too! Therefore the phone still had some commercial value, as it would function on at least 3 out of the 4 networks.

It wasn't long before Orange and T-Mobile began to combine their individual blacklist databases. Therefore a phone barred on Orange was also barred on T-Mobile and vice versa. Even at this point the barred handset could be unlocked and used but only on 2 out of a possible 4 networks (O2 & Vodafone). The government eventually stepped in and forced O2 and Vodafone to update their systems and introduced the CEIR. Now that all the networks share a central blacklist database, even if a barred handset is unlocked it still remains useless on ALL UK networks!

e) How Do Criminals Get Around The Blacklisting Scheme/CEIR?

So now that handsets are blacklisted on all networks what do the criminals do to get around this? They find ways to change handset IMEI numbers! Amazingly it is only recently that the altering/changing of IMEI numbers has become illegal! Home Secretary David Blunkett introduced a new law making re-programming IMEI numbers punishable by up to five years in jail. This new law became active on the 4th October 2002. (This new law does not affect handset unlocking). Never the less it is possible to change IMEI numbers on certain handsets. So if an individual obtains a blacklisted handset, they can change the IMEI number and the handset will then work again!! In my opinion the responsibility now lies with the handset manufactures. They need to make it as difficult as possible to change IMEI numbers. To be fair some manufactures are doing their bit (but some are not!). For example Nokia's older DCT 3 range of handsets has been well and truly cracked. Anyone that searches the Internet for a short period of time would be able to find an IMEI change solution. But Nokia's new DCT4 range of handsets remains UN beaten with regards to changing the IMEI. This is largely down to the type of memory used to store the IMEI number. Nokia have chosen to use OTP (one time programmable) memory, which by its very name indicates that data can't be over written. (Unless you change the UEM/memory chip - technically this is out of the realms of most criminals!). The criminals do have an alternative to changing IMEI's, and this is to send the barred handsets overseas! The blacklist database (or CEIR) is only used by the UK networks. Therefore a handset that is barred in the UK will work fine in a different country! Apparently a large number of UK barred handsets find themselves in Italy, Spain and France etc. The Barred handset works fine in any country outside the UK!! The solution to this exporting problem is simple. Rather than a national database the mobile industry is now looking to build an international database. If/when this is introduced blacklisted handsets will not work anywhere in the world!



(Figure : 2 Before Sniffer Detection)

VII. DESIGN FOR THE SNIFFER

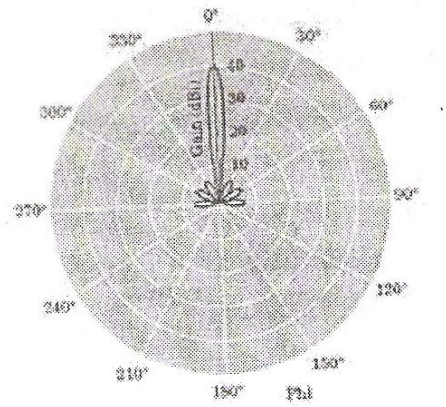
The sniffer for the mobile includes the mobile includes the following important concepts.

- Design of a sniffer base station.
- Design of unidirectional antenna.
- Software that is used for tracking the lost mobile phone's IMEI number.

a) The design for sniffer base station:

- The sniffer is a small base station; it includes transmitter and receiver circuit.
- It should operate at a frequency that is much different from the frequency that is being operated by the operator in the current cell and the near by one's.
- In addition to this the main other requirement is the design for highly powerful unidirectional antenna with very low beam width.
- The design for base station is an important requirement. Mobile phones as well as the base station has low power transmitter is also transmitting at low power.
- The transmitter of the **"*sniffer*"** can be low power transmitter.
- This helps in the process of reducing the interference of the device with the devices that are in the other cells.

b) Design of a unidirectional antenna.



(Figure.3.The Unidirectional Antenna Pattern)

- Though the trans receiver in a sniffer plays an important role in the direction of mobile phone but however it is the directional antenna that has a major role in the design of a transmitter. Hence the proper design of a directional antenna is required.
- Antenna is a device which works on a specified frequencies range for transmitting or receiving the data signals.
- In general, an antenna transmits more power in some directions then in others.
- In addition to this it is necessary that the transmitter should be a low power transmitter.
- Gain and directivity are intimately related in antenna.

- The directivity of 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 it is distributed over a 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 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 it is a slice taken horizontally through the three dimensional sphere.

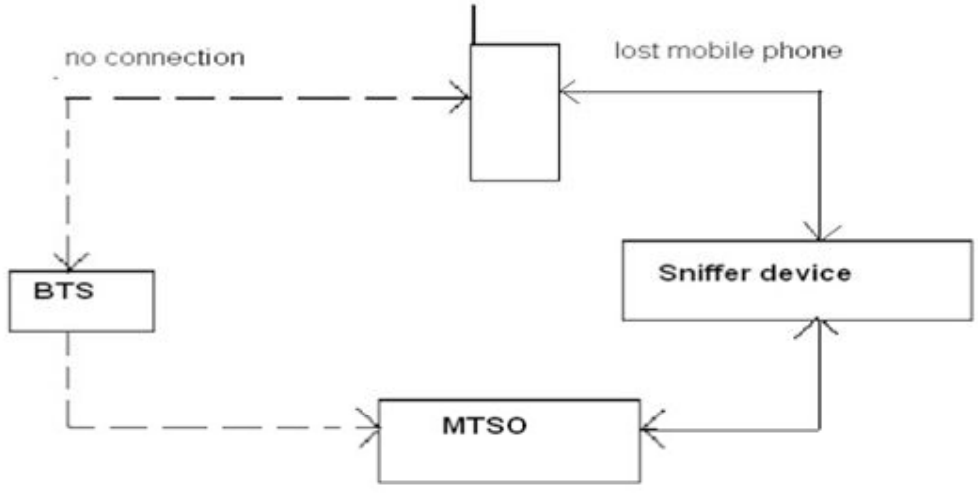
c) Software for the tracking:

- The software part also plays a major role in the tracking of the lost mobile phone.
- The mobile phone that is lost has certain IMEI number that is embedded into the chip.
- The software that is to be designed in such a way that the software has the input as the IMEI number of the lost mobile phone.
- After getting the input of the lost mobile phone's IMEI numbers it checks the common port for getting the information weather the information is available in regard to the lost IMEI number.
- In this way the software gets the information from the antenna, to detect the lost mobile phone.
- The programming can be done with C or JAVA with VB and Oracle at the back end providing the data base information.

VIII. WORKING OF SNIFFER DEVICE:

- The sniffer is a trans receiver that works on the frequency that is in special unused range that is operated by the service provider.
- The fig 2 and 4 shows the working of the sniffer, the first one gives the normal connection of the lost mobile phone with the cellular network.
- First the IMEI of the lost mobile phone has to be reported to the service provider, who keeps in track of the record of the lost mobile phones.
- Then the MTSO which keeps it to track of all mobile phones, their IMEI numbers, their location under which cell, under which BTS

The next fig shows the sniffer that gets in to work. After the information is provided by the MTSO; the sniffer located in the particular cell gets into action by detecting if the mobile phone is available. The base station disconnects the connection with the lost mobile phone while the connection between the sniffer and mobile phone is established; the sniffer is operated in the frequency that is different from the frequency from the frequency adopted by the cell and the near by ones. Hence the interface from the nearby cell can be avoided. The directional antenna is used for the purpose of finding the location of the mobile phone.



(Figure:4 Sniffer Detection For Lost Mobile)

Here the antenna pattern is plotted ones the signal of the mobile phone is obtained. The number of antenna pattern for different position of the same mobile phone is used to find the exact location, but however in this method the directional antenna used must be of very small beam width.

IX. MERITS AND DEMERITS:

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

X. CONCLUSION

Sniffer 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] http://www.infoworld.com/articles/tc/xml/01/12/03/011203tcpackets.
[3] Mandy Andress, 2001 (get to know your network.htm).http://online.securityfocus.com/infocus/1549.
[4] MathiewTanase, 2002 (SecurityFocus Home infocus Sniffers what they are and how to protect yourself.htm).
[5] http://123seminarsonly.com/Seminar-Reports/043/78605740-Whitepaper.pdf
[6] http://www.itpathshala.com/forums/showthread.php?114-Detection-of-lost-mobile-Seminar-reports-amp-ppt-downloads-for-btech-students&s=f857b08ed3ab10cbccb934bd46895500
[7] Schiller, "Mobile Communication", Pearson Education 1 Edition, 7th reprint -2003. •
[8] 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. •
[9] uthiyavan,U., "Enhancing User Privacy- Location Based Search Using MEMD" , IEEE International Conference on Portable Information Devices 2007, May 2007, Pp-1-5.
[10] Ansari, S., Rajeev, S., & Chandrashekar, H. (2002). PacketSniffing: A Brief Introduction. IEEE Potentials (Vol. 21, Issue 5,pp. 17-19).
[11] 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)
[12] .Dhar, S. (2002). "Switchsniff". Retrieved from http://www.linuxjournal.com/article.php
[13] Flor, N.V. & Guillory, K. (2011). Technology Corner: InternetPacket Sniffers Journal of Digital Forensics, Security and Law,Vol. 6(1).
[14] Fuentes, F. & Kar, D. (2005). "Ethereal vs. Tcpdump: A Comparitive Study on Packet Sniffing Tools for Educational
[15] Purpose," Computer Journal of Computing Sciences in Colleges,(Vol. 20, Number 4, pp. 169-176)..
[16] Muna, M., Jawhar, T. & Mehrotra, M. (2010). System Design for Packet Sniffer using NDIS Hooking, International Journal of Computer Science & Communication (Vol. 1, No. pp.171-173).
[17] Niphadkar, S. (2006). *Analysis of Packet Sniffers – TCPdump VS Ngrep VS Snoop*
[18] Spangler, R. (2003). Packet sniffer detection with antisniff. Retrieved from http://www.linuxsec.net/Sniffer.Detectors/snifferdetection.pdf
[19] Wikipedia. (2012). *Packet Sniffer*. Retrieved from http://en.wikipedia.org/wiki/Packet_sniffer