Sniffer for Detecting Lost Mobiles

Dr. B. N. Shobha[1], Ravi MV[2], Sneha B[3]

Professor and HOD, Department of Electronics and Communication[1]

Assistant Professor, Department of Electronics and Communication[2]

Student, Department of Electronics and Communication[3]

SJC Institute of Technology, Chikkaballapura, India

Abstract: *The main goal of this Endeavour is to use sniffer technology to track down a misplaced cell phone. Regularly thousands of adaptable get misplaced. Security for mobile devices is necessary since portable companies are now building mobile devices with IMEI to locate the mobile device, but this system is not very effective. Hence, sniffer technology is applied. This device, which combines a Sniffer Base Station, an Unidirectional Antenna, and Tracking Software, can be referred to as a Base Station. To maintain the recurrence, the Sniffer Base Station is used. Recurrence is a VHF extension at 900 MHzTo exchange the flag relating to the desired recurrence for receiving and transmitting signals, unidirectional radio wire is employed. The most important component of cell phone monitoring is the programming. Because of the way this programming is laid out, the IMEI of the device is read from its Memory. It checks for a signal from a device that responds to a flag sent by sniffer technology. The IMEI number, which stands for "International Mobile Station Equipment Identity," identifies a device that uses GSM technology*.

Keywords: Sniffer, BTS, MSC, IMEI, IMSI

I. INTRODUCTION

The primary purpose of a sniffer is to find misplaced mobile devices. Every day, thousands of mobile phones are misplaced or lost. Although the manufacturers of the mobile devices have implemented an effective method to block the lost mobile to stop unauthorized individuals from placing and receiving calls, there has been very little advancement in the field of misplaced mobile phone detection. SNIFFER is essential for finding misplaced mobile devices.

For the purpose of detection, the sniffer equipment needs to be precisely sized and reduced in size for easy mobility. The gadget, which has a unidirectional antenna, tracking software, and a sniffer base station, can be referred to as a mobile base station. A small base station called a sniffer has a transceiver portion. It should operate at a frequency that is significantly lower than the frequency of the present cell, which is where the detection operation is being run. The directional antenna is a crucial component that must be constructed and used since it has a crucial function.

There are various technologies available for capturing network traffic, however some of them have drawbacks. The researcher must utilize other tools for analysis to obtain the necessary traffic features and take the memory size of the system in use into account because some tools merely capture network traffic without analysis while others demand huge memory sizes for installation. Our technology records and examines network data, allowing the user to select only the functions he requires. Our solution allows the user to save their chosen features in a file for subsequent use in their work and takes little memory space for installation. As a result, less RAM will be required to store the data.

II. LITERATURE REVIEW

1.Abdelallah and Elhad (2020)In their research work, they came to the conclusion that the sniffer combines looking for machines operating promiscuously with utilising a honeypot to detect the use of sniffer data. Sniffer includes all platform detection that occurs online as well as detection that occurs after information replay. Furthermore, detection based on MAC addressing enables the identification of any network device operating in promiscuous mode on any Linux or Windows platform.

2.Remo and Ogun (2021) This study came to the conclusion that there are numerous techniques available for capturing network traffic, however some of them have drawbacks. Without analysis, some tools just record network traffic, and

others need a lot of memory to install, so researchers must utilise other tools to obtain the necessary traffic features while also taking the system's memory requirements into account. This system records network traffic, analyses it, and gives the user the tools he requires. This method allows users to save particular features in a file or document for later use in their work and requires little memory space for installation. This will decrease the amount of RAM needed to store data.

3.Patil at el. (2019) They suggested in their research paper that an Android app had been developed and integrated into the phone's foundation for tracking down stolen or misplaced mobile devices. The built-in GPS in mobile phones helps this application function. When an anonymous client tries to switch a wireless device's SIM card to a predefined portable number without the client's knowledge, the current longitude and scope data are transmitted as an SMS. Google Maps can be used to locate the exact location. Utilising the scope and longitude values.

4.Lomet at el. (2020)provided their opinion that, if you are already a Sniffer customer, you are unaware of additional security features that can be used to supplement your security precautions. Additionally, the capacity to reshape current innovations in novel ways offers incredible budgetary controls for enhancing system security performance. Before, during, and after an attack, Portable and Distributed Network Associates can provide customers with more than just increased system performance and uptime; they can also assist in securing your system infrastructure. To provide clients with solutions for their system, board, and security, Sniffer Technologies employs organize examination aptitude.

III. METHODOLOGY

The designing process can be done by using three mainly important components:

- Sniffer base station,
- Unidirectional antenna
- Software for tracking

Sniffer functions as a miniature base station. It functions as a transceiver part. It ought to run at a frequency that is distinct from the one used for the detecting procedure. Some of the most crucial elements are the frequency that the transceiver section must produce, which is in the VHF range and utilised to construct the oscillator. This frequency is in the region of 900 MHz. As is well known, both base stations and mobile devices have weak transmission powers. Because of this phenomena, we are able to reduce device interference.

The antenna serves as the detecting process' eye.A device called an antenna is used for sending or receiving signals. Depending on the power or directivity of the antenna, its lobe pattern determines how much power it can send.When the directivity is high, the directional gain is also at its highest on the same side. Directivity is defined as the maximum direction gain. It might switch from one antenna to another. In all directions and for all antennas, the directivity value remains constant. Another crucial element that is primarily necessary for the detection process and is dependent on the area that has been captured with a high degree of directivity is the effective area.

The tracking procedure also makes use of the software. It creates a connection between our sniffer device and any missing gadgets. Because the IMEI number is included into the software, it serves as the database or directory for the missing device. Software collects the signaling information provided by the antenna after receiving the IMEI number and after checking the information available worldwide. Either the "C" or "JAVA" programming languages are used, but we prefer the "C" programming language because it is more convenient and preferable on chips.

IV. WORKING OF THE SNIFFER DEVICE

The sniffer is essentially a transceiver that operates in a frequency that is significantly different from the one being used by the nearby cells because there may be a chance of interference between the device and the devices in the nearby cells. It can also be designed to operate at a frequency that is in a special unused range that is operated by the service provided. The device operates in the manner described below. It allows the mobile to function normally with the base station, and there is a BTS that serves as a go-between in the communication process between the mobile and the MTSO, also known as the MSC or Mobile Switching Center.There is always two-way communication between the devices, and before that can happen, the SIM card must be authenticated since it has an IMSI, or international mobile subscriber identifier. The user's authorization is aided by this IMSI number. The handset is verified in the EIR, or

Equipment Identifier Register, as the second authentication. If the signal is obtained from the regular one, two-way contact is established. This register is located at the MSC and it contains the IMEI number of the lost device. A lost mobile phone's IMEI has previously been reported to the service provider, who keeps track of lost mobile phone records.Due to two-way communication with the device, the MSC is aware of the BTS of the lost device. The MTSO or MSC, which keeps track of all mobile phones with IMEI numbers and IMSI numbers, has information about the location of lost mobile phones, which means the location of the cell where the lost device is. The sniffer device is introduced based on this knowledge of the cell in which the device is positioned.
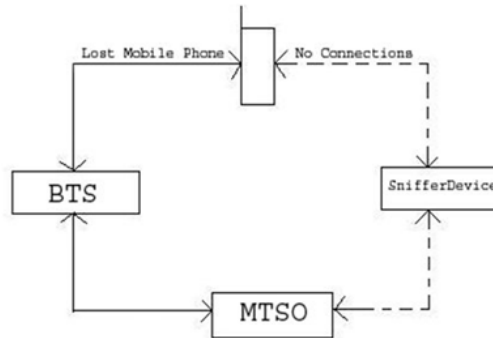

Fig 1: Before Sniffer increases the frequency

The sniffer that begins to search for a lost device is shown in the following figure. following the MTSO or MSC's provision of the lost device's IMEI number information. This is then input into the sniffer's main memory, and the sniffer that is located in that particular cell begins to work on finding the missing device. The sniffer operates on a frequency distinct from the one thatis utilised by the base station as well as the close-by cells. Following a request for this step from the EIR section of the MSC, the base station cuts off communication with the missing mobile phone. Due to each base station's lack of authorization capabilities, this forces the lost device to search the BTS in order to get locked, causing it to transmit the proper connection request signal. Now, when the sniffer device is deployed and equipped with built-in authorization capabilities, the lost device locates the sniffer and locks onto its frequency. During the establishment of the connection between the mobile phone and the sniffer; once successful permission, communication is established between the sniffer and the lost device once the IMEI of the lost mobile device is verified against the saved IMEI. When the IME is validated, access is prohibited to the sniffer if any other devices connected to it attempt to communicate with it. Once communication has begun, the antenna and signal strength of the lost device are mostly used to determine where it is. However, the GPS system can also help with the search process for a more precise and quick detection. The primary need is that the sniffer be operated at a frequency different from those used by the cell and cells nearby.
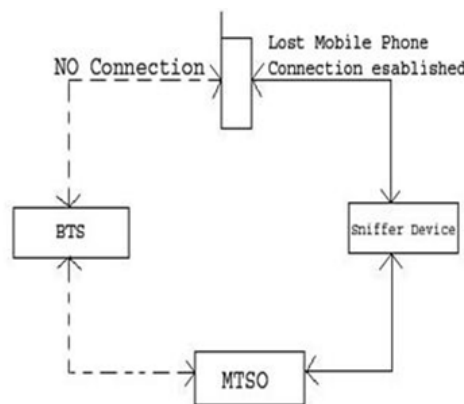

Fig 2: After Sniffer increases the frequency

20

V. APPLICATIONS AND ADVANTAGES

5.1 APPLICATIONS

A sniffer is a programmed that watches and examines network traffic in order to find bottlenecks and other issues.

- A network administrator can efficiently maintain traffic flow by using this information.
- Sniffers can be used legally or illegally to record data that is being transmitted over a network. A network router reads each packet of data that is sent to it and determines whether it should be forwarded farther via the Internet or to a destination within the router's own network.
- However, it's possible for a sniffer-equipped router to read both the source and destination addresses and the contents of the packet.
- In order to avoid traffic snarls brought on by filesharing programs, sniffers are frequently utilised on academic networks.

5.2 ADVANTAGES

- Cost Effective
- Low power Consumption
- Easy to Design
- This Method is used for finding lost mobiles effectively.

VI. CONCLUSION

One of the most popular devices in the sphere of communication since technological growth is the mobile phone. Many mobile phones are forgotten or lost for various causes, hence this study serves as the foundation for the Sniffer Technology for Detecting Mobile Phones. Sniffer base station, unidirectional antenna, and software for tracking procedure were the three primary parts we used for this process. The antenna's design is crucial because detection is correctly dependent on signal intensity or directivity, with detection occurring in the same general direction as where the signal strength is greatest.

VI. FUTURE SCOPE

The power of the mobile phone should be sufficient, it shouldn't be in the shadow region, etc. are some of the boundary requirements or criteria that must be met for the identification of the lost mobile. But, this approach can be enhanced by employing current technologies and equipment.

REFERENCES

[1]. Abdelallah and Elhad, "Searching for machine in promiscuous mode", Computer Journal of Computing Sciences in Colleges, 2020, pp. 169-176.

[2]. Remo and Ogun "Tools to capture network traffic", JournalofComputerand Communications,2021, pp. 164-173.

[3]. Sharangouda J. Patil1, Sneha R. Banagar, Ravikumar R. Banagar, S. Venkatesh, T. Vishwanatha and Saraswati B. Patil, "Sniffer to detect mobile tracking", in Proc. IEEE 17th Int. Conf. Comput. Supported Cooperat.WorkDesign(CSCWD),Whistler,BC,Canada,Jun.2019,pp.651–657.

[4]. Lomet, B. M. Pang, H.S. Shi, "Sniffer client", Journal of Future Wireless Networks and Information Systems, vol. 143, , 2020,pp. 163–170.

[5]. Arvind and Negi, "Sniffer Assistant", 2018 International Journal ofEngineering& Technology,vol. 7, no.3, 2018, pp. 226-228.

[6]. Asrodia, P. & Patel, H. "A Comparitive Study on Packet Sniffing", International Journal of Engineering Research and Applications, Vol. 2, 2012, pp.854-856.

[7]. P.Koopman," System Design for Packet Sniffer using NDIS Hooking ",IEEEComputer,vol.37,no.7,2020,pp.95-97.

[8]. S. Ravi, A. Raghunathan, P. Kocher and S. Hattangady," Packet sniffer detection with antisniff", ACM Transactions on Embedded ComputingSystems,vol.3,no.3,2021, pp. 461-491.

[9]. D. Bhowmik and K.Appiah," Sniffer Technology to Detect Lost Mobile ",Proc. Int.Symp. Appl. Reconfigurable Comput., pp. 204-216,2018.

[10]. Mathiew Tanase," Enhancing User Privacy- Location Based Search Using MEMD",Proc. Int.Symp. Appl. Reconfigurable Comput., pp. 204-216,2019.

[11]. A. Bhandari, S. Gautam, T. K. Koirala and M. R. Islam, "Packet Sniffing and Network Traffic Analysis Using TCP-A New Approach" in Advances in Electronics Communication and Computing, Springer, pp. 273-280, 2018.

[12]. M. A. Qadeer, A. Iqbal, M. Zahid and M. R. Siddiqui, "Network traffic analysis and intrusion detection using packet sniffer", Communication Software and Networks 2010.ICCSN'10.Second International Conference on, pp. 313-317, 2010.

[13]. P. Asrodia and H. Patel, "Analysis of various packet sniffing tools for network monitoring and analysis", International Journal of Electrical Electronics and Computer Engineering, vol. 1, pp. 55-58, 2012.

[14]. J. Yang and Y. Zhang, "RTT-based Random Walk Approach to Detect Stepping-Stone Intrusion", Proc. of 29th IEEE International Conference on Advanced Information Networking and Applications, pp. 558-563, March 2015.

[15]. Rajesh Kumar, S Niranjanr and Yashpal Singh, "A Review on Mobile Agent Technology and Its Perspectives", Journal of Computer Sciences and Applications, vol. 3, no. 6, 2015.

[16]. Amit Mishra and AnamikaChoudhary, "Mobile Agent: Security Issues and Solution", International Journal of Computer Technology and Electronics Engineering (IJCTEE), vol. 2, 2012.

[17]. Allan Brimicombe and Yang Li, "Mobile Space- Time Envelopes for Location-Based Services, Transactions in GIS, Vol. 10, No. 1 pp. 523, 2006.

[18]. E. Vattapparamban, B. S. Ciftler, I. Guvenc, K. Akkaya, and A. Kadri, ''Indoor occupancy tracking in smart buildings using passive sniffing of probe requests,'' in Proc. IEEE Int. Conf. Commun. Workshops (ICC), May 2016, pp. 38–44.

[19]. A. Basalamah, ''Crowd mobility analysis using WiFi sniffers,'' Int. J. Adv. Comput. Sci. Appl., vol. 7, no. 12, pp. 374–378, Dec. 2016.